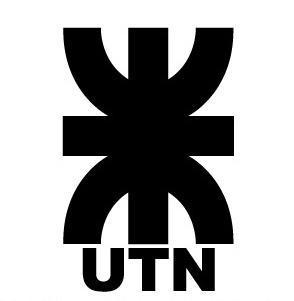
**UNIVERSIDAD TECNOLÓGICA NACIONAL**

Facultad Regional Resistencia

****

Ingeniería en Sistemas de Información

**Cátedra: Administración de Recursos**

Materia integradora del 4to nivel

**Trabajo Práctico 6.1:** “Seguridad de SI

**Profesores:**

• **Responsable de Cátedra:** Ing. Claudia A. SORIA OJEDA

• **Jefe de Trabajos Prácticos:** Ing. Rosina RAMIREZ

• **Auxiliar Docente:** Ing. Jorge ROA

**Grupo N°: 2**

**Alumnos:**

* Bellini, Maximiliano
* García, Emmanuel
* Ortega, Fernanda
* Peressi, Gonzalo
* Zaracho, Santino

**2019**

**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:**

**a) Identificar las vulnerabilidades, amenazas y riesgos referidos en el artículo.**

* Se puede considerar que los empleados de una empresa X, cuentan con dispositivos Android, terminales con Linux y OpenBSD (que son más susceptibles a este ataque que Mac o Windows) y que se conectan por medio de un AP o router de la empresa utilizando WPA2 como medida de seguridad.
* Se puede considerar también que el atacante está en las proximidades (ej: en un bar, automóvil, plaza).

**Síntesis del ataque:** Key Reinstallation AttaCK se logra mediante la utilización de un AP “Falso” o “Clon” para engañar al cliente, entonces el mecanismo de WPA2 **no utiliza la clave real de encriptación al establecer nuevamente la comunicación con el verdadero AP, en lugar de ella, usa una genérica de ceros,** lo cual da acceso a todo el tráfico dentro de la red sin estar dentro de ella, además de ello se usa otro mecanismo para anular el cifrado SSL (ya conocido), permitiendo ver información de sitios que trabajan con aquel mecanismo. Lo que impresiona de esto, es que antes no era posible observar el tráfico de la red sin estar autenticado en ella (había que conseguir la clave mediante handshake y fuerza bruta o diccionario), ahora, con la falla mencionada al principio, es posible hacerlo.

**Elementos amenazados conectados a una red usando WPA2:**

* Ordenadores con SO Linux u OpenBSD, y en menor medida Windows y MacOS X.
* Dispositivos Android.
* Routers y Access Points (Mediatek-Linksys).

**Vulnerabilidades:**

* Falta de conocimiento del los empleados sobre seguridad en sitios (con/sin seguridad HTTPS).
* SO Android que permite cambiar el AP por medio del envío de ciertos mensajes.
* Debilidad en la seguridad de WPA2 a ataques del tipo “man in the middle”.
* Sitios web que tienen errores en su configuración de HTTPS.

**Amenazas:**

* Ataque KRACK sobre los dispositivos Android u AP de la empresa (afecta confidencialidad).
* Infección de virus-ransomware (afecta integridad, disponibilidad y confidencialidad).
* Ciberespionaje (afecta confidencialidad).

**Riesgos:**

* Probabilidad de que un dispositivo android sea víctima de un ataque del tipo KRACK.
* Probabilidad del robo de información sensible de la empresa o de la persona por medio de los dispositivos Android comprometidos.
* Probabilidad de que producto de la pérdida de confidencialidad de los dispositivos Android se produzca un ataque que afecte la disponibilidad o integridad de la información de la empresa, y/o del dispositivo en cuestión.

**b) Clasificar las amenazas identificadas, indicando, además, si son ataques pasivos o activos.**

**Ataques pasivos:** En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo transmitida.

**Ataque Activo:** Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos.

|  |  |  |
| --- | --- | --- |
| **Amenaza** | **Tipo** | **Ataque** |
| KRACK | Lógica-Deliberada | Activo (suplantación de identidad y modificación de mensajes) |
| SSLStrip | Lógica-Deliberada | Activo (suplantación de identidad y modificación de mensajes) |
| WireShark | Lógica-Deliberada | Pasivo (monitoreo de tráfico) |
| Ciberespionaje sobre dispositivos  Android | Lógica-Deliberada | Pasivo (monitoreo de tráfico) |
| Infección de Virus o ransomware | Lógica-Deliberada | Activo |

**c) Identificar y redactar adecuadamente las políticas y medidas enunciadas.**

A partir de los siguientes extractos de los artículos y/o links que aparecen en este, **se producirán las políticas de seguridad que consideramos más importantes:**

* Afortunadamente, si el tráfico WiFi se encuentra cifrado ya que el usuario se encuentra navegando por una página con el protocolo de seguridad HTTPS u operando bajo una conexión VPN, un ciberatacante no podría interceptar la comunicación.
* *«Una vez que sepamos los detalles de la vulnerabilidad los fabricantes tendrán que lanzar parches «firmware» y actualizarlos»*, explica. Pero hay un problema añadido: no todos son actualizables. Es más, la gran mayoría de los routers existentes no se puedan parchear rápidamente y es posible que algunos no se pueda hacer en absoluto. *«El problema es que muchos puntos de acceso no podrán ser parcheados sobre la marcha con lo que usar WiFi puede ser inseguro en la mayor parte de los escenarios».*
* En su opinión, navegar en cualquiera de las redes WiFi expone, de manera automática, *«nuestra seguridad»* y *«los datos que manejamos»*. *«Una demostración más de que lo que hoy es seguro mañana puede no serlo porque la tecnología está hecha por humanos, que somos susceptibles de equivocarnos»*.
* Vanhoef said clients can be patched to prevent attacks even when connected to vulnerable access points. Linux patches have been developed, but it's not immediately clear when they will become available for various distributions and for Android users. Patches are also available for some but not all Wi-Fi access points. We need for a WPA3 standard, Vanhoef wrote:No, luckily [WPA2] implementations can be patched in a backwards-compatible manner. This means a patched client can still communicate with an unpatched access point, and vice versa. In other words, a patched client or access points sends exactly the same handshake messages as before, and at exactly the same moments in time. However, the security updates will assure a key is only installed once, preventing our attacks. So again, update all your devices once security updates are available.
* **If possible, people with vulnerable access points and clients should avoid using Wi-Fi until patches are available and instead use wired connections. When Wi-Fi is the only connection option**, **people should use HTTPS, STARTTLS, Secure Shell, and other reliable protocols to encrypt Web and e-mail traffic as it passes between computers and access points**. As a fall-back users should consider using a virtual private network as an added safety measure, but users are reminded to choose their VPN providers carefully, since many services can't be trusted to make users more secure.

**Teniendo en cuenta que:**

Una política de seguridad puede ser **prohibitiva**, si todo lo que no está expresamente permitido está denegado,o **permisiva**, si todo lo que no está expresamente prohibido está permitido. Evidentemente la primera aproximación es mucho mejor que la segunda de cara a mantener la seguridad de un sistema; en este caso la política contemplaría todas las actividades que se pueden realizar en los sistemas, y el resto - las no contempladas - serían consideradas ilegales.

Cualquier política ha de **contemplar seis elementos** claves en la seguridad de un sistema informático:

* **Disponibilidad:** Es necesario garantizar que los recursos del sistema se encontrarán disponibles cuando se necesitan, especialmente la información crítica.
* **Utilidad:** Los recursos del sistema y la información manejada en el mismo ha de ser útil para alguna función.
* **Integridad:** La información del sistema ha de estar disponible tal y como se almacenó por un agente autorizado.
* **Autenticidad:** El sistema ha de ser capaz de verificar la identidad de sus usuarios, y los usuarios la del sistema.
* **Confidencialidad:** La información sólo ha de estar disponible para agentes autorizados, especialmente su propietario.
* **Posesión:** Los propietarios de un sistema han de ser capaces de controlarlo en todo momento; perder este control en favor de un usuario malicioso compromete la seguridad del sistema hacia el resto de usuarios.

Políticas de seguridad que inferimos podríamos aplicar según entendemos de estos consejos:

**Propósito:** Esta política proporciona un conjunto de procedimientos y estándares para implementar tecnologías inalámbricas dentro del entorno de red. Proporciona a los administradores de red que implementan y administran estas tecnologías un conjunto básico de requisitos que documentan la conectividad, la seguridad y la supervisión del dispositivo.

**Alcance:** Esta política se aplica a todo el personal que diseña, instala y ofrece soporte a redes inalámbricas.

**Autenticación y Transmisión (prohibitiva-Autenticidad):** Todos los puntos de acceso inalámbrico que conectan clientes a la red interna (LAN) requerirán que los usuarios proporcionen autenticación única a través de canales seguros, y todos los datos transmitidos se cifran según la tecnología de encriptación aprobada por el área de seguridad de IS.

**Localización física (prohibitiva-Posesión):** Deben establecerse mecanismos de seguridad para evitar el robo, la alteración o el mal uso de puntos de acceso/estaciones base. Todos los dispositivos deberán estar bloqueados y asegurados de manera adecuada.

**Tecnología aprobada (prohibitiva-Posesión):** Todo terminal, dispositivo o hardware de LAN inalámbrica usado para conectarse a una red deberán ser configurados para usar las últimas actualizaciones de seguridad disponibles.

**Registrar puntos de acceso (prohibitiva-Posesión):** Todos los puntos de acceso inalámbricos/ estaciones base conectados a la red deben estar registrados y aprobados por el área de seguridad de IS. Todos los puntos de acceso/estaciones base aprobados están sujetos a pruebas y auditorías periódicas de penetración.

**Aplicación (prohibitiva-Confidencialidad):** Cualquier empleado que por sus tareas o funciones establecidas, haya violado las políticas de seguridad vigentes, por acción u omisión, estará de estar sujeto a medidas disciplinarias que pueden incluir terminación del empleo.

**d) Clasificar las medidas indicadas.**

|  |  |
| --- | --- |
| **Medida** | **Clasificación** |
| El acceso a los sitios a internet se limitará a sitios que tengan configurado correctamente HTTPS. | Preventiva |
| Toda comunicación o información sensible tendrá una capa de encriptación adicional. | Preventiva |
| Se establecerá un control de acceso sobre las personas que ingresan a la empresa para el registro y control de los dispositivos. | Detección |
| Los equipos de seguridad ejecutarán pruebas de penetración periódicas para evaluar vulnerabilidades, nuevas amenazas y los riesgos que representan para la infraestructura de IS de la empresa. | Preventiva |
| Se generará un registro de todos los HW y SW pertenecientes a la infraestructura de IS, el cual contará con la información adecuada que permita una rápida identificación de los mismos, como también de las últimas actualizaciones de seguridad ofrecidas por el fabricante para cada elemento. | Prevención |

**2. Leer detenidamente el artículo *“***[***Telefónica y otras empresas españolas sufren un ciberataque en sus redes internas***](https://www.abc.es/tecnologia/redes/abci-telefonica-sufre-ciberataque-interna-201705121304_noticia.html)***”*. Luego:**

**i) Realizar la etapa de identificación de riesgos (vulnerabilidades, amenazas, elementos amenazados y riesgos).**

|  |  |
| --- | --- |
| **Management de la seguridad de los IS** | |
| Etapa 1 : | IDENTIFICACIÓN DE RIESGO |

**Vulnerabilidades:**

* Fallo de seguridad en algunas versiones del sistema operativo Windows instalado en las computadoras de Telefónica.
* Falta de capacitación del personal sobre la apertura de correos electrónicos de fuentes no confiables.
* Vulnerabilidad de ejecución de comandos remota a través de SMB (protocolo de red que permite compartir archivos), se distribuye al resto de ordenadores Windows que haya en esa misma red.
* Cantidad o falta de tiempo que permita al equipo de seguridad realizar un management de riesgo sobre una nueva vulnerabilidad desde el momento en que es descubierta o anunciada, hasta que esta puede ser utilizada para un ataque **(2 mes aprox. en el caso de Telefónica).**
* Falta de inmediatez entre que se declara una vulnerabilidad en Windows que afecta a los equipos de la compañía y el lanzamiento de los parches de seguridad correspondientes.

**Amenazas:**

|  |  |  |
| --- | --- | --- |
| **Amenaza** | **Tipo** | **Ataque** |
| Infección de Ransomware, virus, malware | Lógica- Deliberada | Activo |
| Errores en el equipo de seguridad en el management de riesgo que permita tomar medidas rápida y eficientes ante amenazas emergentes. | Lógica- Accidental | Activo |
| Errores del personal en el uso del ordenador, dejando expuesta la infraestructura de sistemas a las amenazas de internet. | Lógica-Accidental | Activo |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Elementos Amenazados** | | | | |
| **Equipamiento bajo riesgo en el área de la red interna de Telefónica:** | | | | |
| **Recurso** | **Cantidad** | **Valor unitario** | **Valor Total** | **Descripción** |
| Equipo PC | 100 | $18.000 | $1.800.000 | Ordenadores que utilizan en los puestos de trabajo los  empleados del área de la red interna de Telefonica. |
| **Infraestructura asociada a los equipos comprometidos:** | | | | |
| * Impresora: Plotter Canon Ipf670s 61 cm * Scanners: Epson Perfection V600 * AP: Ubiquiti Uap Ac Lr | 5, 5 y 4, respectivamente | $70.000, $23.000 y $9.000, respectivamente | $40.000, $155.000 y $32.000, respectivamente | Infraestructura que pudo haber sido comprometida por otras amenazas y por lo tanto requiere ser evaluada. |
| TOTAL |  |  | $2.027.000 |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Elementos Amenazados** | | | | |
| **Informacion bajo riesgo área de la red interna de Telefónica.** | | | | |
| **Recurso** | **Cantidad** | **Valor unitario** | **Valor Total** | **Descripción** |
| Datos personales de  clientes comprometidos | 700  (suponiendo que cada empleado maneje con su ordenador una cartera de 7 clientes, 100 \* 7 = 700) | $150.000  Suposición: En concepto de pago de sentencias + costas legales | $105.000.000 | Datos personales correspondientes a los clientes con los que trabaja el área de la red interna de Telefónica. |
| Documentos de trabajo del día del ataque sin backup | 700 cómo mínimo | $5000  En concepto de horas extra para volver a contactar a los clientes e interrupción del día de trabajo | $350.000 | Pérdida de trabajo e información del dia del ataque |
| TOTAL |  |  | $105.350.000 |  |

|  |  |  |
| --- | --- | --- |
| **Elementos Amenazados** | | |
| **Elementos bajo riesgo intangibles** | | |
| Es difícil evaluar (cuantitativa y cualitativamente) los elementos amenazados por este tipo de amenazas**,** pero tanto los **empleados** que abrieron un correo desconocido infectado, como la falta de medidas que el **equipo de seguridad** (que pudo haber tomado luego de casi 2 meses de anuanciada la vulnerabilidad en el SO de Windows) fueron las **causas de que un riesgo se haya materializado en un ataque.** | | |
| **Recurso** | **Valor Total** | **Descripción** |
| Imagen de la empresa  Confianza de los clientes  Confianza de los inversionistas | **Es difícil estimar el daño primario y más aún el secundario en estos factores.**  **Pero un claro indicador sería la pérdida en las acciones en la bolsa que registró Telefónica del 0,15% que figura en artículo el cual si es cuantificable.**  **Capitalización bursátil €38.000.000.**  **La pérdida del 0,15% representa un valor de €5.320.000, o sea en pesos: $3.648.000** |  |

|  |  |  |
| --- | --- | --- |
| **Riesgos identificados limitados al escenario** | | |
|  | **Deliberado** | **Accidental** |
| Físicos | - | - |
| Lógicos | Probabilidad de que la infraestructura de sistemas sufra un ataque (virus, malware, ransomware) afectando la disponibilidad, integridad o confidencialidad de los datos. | Probabilidad de que el mal uso de un empleado sobre la computadora o internet provoque una infección (virus, malware, ransomware) afectando la confidencialidad, disponibilidad o integridad de los datos.  Probabilidad de que el tiempo de respuesta del equipo de seguridad sea insuficiente para realizar un management de riesgo, y así contrarrestar una o varias amenazas emergentes. |
|

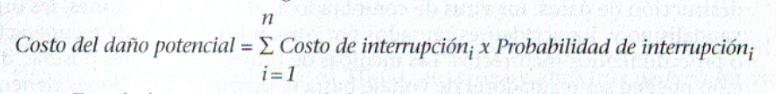
Obviamente pueden existir más riesgos, pero nos limitamos a pensar en los más importantes, dado el escenario planteado. Otros riesgos van desde incendios, robo de equipo, empleados infieles, inundaciones, fallas de energía, etc.

**ii) 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”.**

|  |  |
| --- | --- |
| **Management de la seguridad de los IS** | |
| Etapa 2 : | ANÁLISIS DEL RIESGO |

**Análisis de impacto potencial:**

A continuación se analizará el **Costo de daño potencial** según el **costo de interrupción (i)** y la **probabilidad de interrupción (i)**. Esto se hará para cada riesgo identificado.



|  |  |
| --- | --- |
| **Variable** | **Significado** |
| Costo del daño potencial | Es el monto de pérdida al materializarse los riesgos. |
| Costo de interrupción **(i)** | Es la pérdida potencial de un elemento (activo) evaluado **(i)**.  Fue calculada según los elementos en riesgo según información, dispositivos y RRHH, definidos en el punto anterior. |
| Probabilidad de Interrupción **(i)** | Es una estimación que permite estimar la frecuencia de ocurrencia de cualquier falla de seguridad, a través del producto de la probabilidad de agresión por la probabilidad de que la misma tenga éxito.  Se utilizará el siguiente rango de probabilidades:  **Baja = 0% - 30%**  **Media = 31% - 60%**  **Alta = 61% - 100%** |
| Donde **(i)** es un evento probable. Es un riesgo particular identificado.  Y **n e**s el número de eventos. Es la cantidad de Amenazas identificadas. | |
|

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Amenaza Particular (i)** | **Probabilidad de agresión** | | **Probabilidad de éxito de la agresión** | | **Probabilidad de Interrupción (i)** | **Costo de interrupción (i)** | **Costo del daño potencial** |
| Infección de virus, malware, ransomware  (afecta elementos de información) | ALTA | 85% | BAJA | 30% | 25.5% | $105.350.000 | $26.864.000 |
| Mal uso de un empleado sobre la computadora o internet que afecte la infraestructura de IS de la empresa.  (afecta elementos de equipamiento) | BAJA | 20% | MEDIA | 35% | 7% | $2.027.000 | $141.890 |
| Errores en el equipo de seguridad en el management de riesgo que permita tomar medidas rápidas y eficientes ante amenazas emergentes | BAJA | 8% | ALTA | 85% | 6,8% | $3.648.000 $ | $248.064 |

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Riesgo** | **Pérdida potencial por falla de seguridad** | **Consecuencias primarias** | **Consecuencias secundarias** |
| Infección de virus, malware, ransomware  sobre la infraestructura de IS | * Falla de HW en la infraestructura de IS * Falla de SW en la infraestructura de IS | Pérdida primaria que afecta la disponibilidad, confidencialidad y/o integridad de la información  de la infraestructura de IS afectada.  En nuestro ejemplo, si el riesgo se materializa en un ataque exitoso que afecte tan solo 100 equipos con datos personales de clientes, se espera una pérdida de $26.864.000.  Este ataque causa:   * Interrupción del procesamiento y/o trabajo diario. * Encriptación de los registros de datos. * Revelación de información confidencial. | * Desmotivación de los empleados * Retraso de entregas de trabajos pendientes * Otras áreas dependientes de estas entregas son incapaces de realizar su trabajo * Pérdida de confianza del cliente al enterarse de la noticia * Pérdida de confianza de los inversores → las acciones de Telefónica cayeron en un 0,15% por este incidente. * Incomunicación * Pérdida de posición competitiva * Pérdida del nombre de la empresa |
| Mal uso de un empleado sobre la computadora o  internet que afecte la infraestructura de IS de la empresa, área o equipo. | * Falla de HW en la infraestructura de IS * Falla de SW en la infraestructura de IS * Pérdida de capacidad de procesamiento * Pérdida del trabajo que realiza el personal sobre el equipo propio o sobre la infraestructura de IS. | Pérdida primaria que afecta la disponibilidad, confidencialidad y/o integridad de la información  de la infraestructura de IS afectada.  Esto puede variar e ir desde:   * Interrupción del procesamiento y/o trabajo diario * Incapacidad de seguir con algunas funciones del sistema   En nuestro ejemplo, si el riesgo se materializa, esto puede afectar el equipamiento del área interna de Telefónica (100 terminales + impresoras + escaners + AP) dejándolo ocioso por un total de $2.027.000 | * Otras áreas dependientes de estas entregas son incapaces de realizar su trabajo. * Retraso de entregas de trabajos pendientes |
| Tiempo de respuesta del equipo de seguridad insuficiente para realizar un management de riesgo y así contrarrestar una o varias amenazas emergentes | Supervivencia del negocio | Pérdida primaria que afecta la disponibilidad, confidencialidad y/o integridad de la información  de la infraestructura de IS afectada.  Esto puede variar e ir desde:   * Pérdida de información confidencial * Reducción de la capacidad de procesamiento a corto o largo plazo * Corrupción de información * Destrucción de HW o SW * Detención de las operaciones diarias de la empresa | * Sanciones por inclumplimieto de obligaciones legales * Información Gerencial inútil, imprecisa o desactualizada * Incapacidad de seguir con el negocio * Pérdida de confianza de clientes e inversionistas * Incapacidad de seguir con el negocio * Pérdida del nombre de la empresa |

**iv) Cómo armaría la expresión de “riesgo”, propuesta por Robson?**

La expresión propuesta por Robson dice lo siguiente: *“Para realizar el análisis del impacto potencial se deben tener identificado cada uno de los riesgos cómo su probabilidad de ocurrencia y la gravedad de sus consecuencias”*.

En donde:

* Pérdida esperada ($) = pérdida potencial ($) \* Frecuencia de pérdida
* Frecuencia de pérdida = Probabilidad de Agresión \* Probabilidad de éxito en el ataque

|  |  |  |
| --- | --- | --- |
| **Pérdida esperada ($)** | **Pérdida potencial ($)** | **Frecuencia de pérdida** |
| Por cada amenaza particular identificada | Se realizan cálculos financieros sobre el elemento (activo) que tiene riesgos de ser afectado por una amenaza | **Probabilidad de agresión \* Probabilidad de éxito de la agresión** |

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

Elementos identificados de etapas posteriores:

|  |  |
| --- | --- |
| **Management de la seguridad de los IS** | |
| Etapa 3 : | MANEJO DEL RIESGO |
| Elementos | Las recomendaciones que dan al final del artículo claramente pueden ser consideradas estrategias de manejo de riego que se encuadran dentro de las medidas de reducción de riesgos: **Cómo protegerse ante un «ransomware»**  1. Hacer copia de seguridad: Los expertos recomiendan hacer «backups» o copias de seguridad de manera periodica para evitar perder los archivos importantes y mantenerla fuera del entorno online ante posibles intromisiones ilegales. **(Recuperación)** 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. **(Preventiva)** 3. Tener instalado las actualizaciones del sistema operativo y de los antivirus: es necesario tener todo el software al día para evitar ataques. **(preventiva y detección)** |
| Etapa 4 : | RECUPERACIÓN DEL DESASTRE |
| Elementos | Hay un par de menciones que claramente apuntan a esta etapa:   * *«Lo importante aquí, más que te pase o no, es cómo de preparado estás para recuperarte. Es muy difícil que en una instalación tan grande nadie se vea afectado. Lo que importa es saber hasta qué punto ha afectado a servidores corporativos y esperar que la compañía dé una respuesta transparente y tenga una pronta recuperación».* * *«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».*   Ambas menciones dan cuenta que ningún proceso de management de seguridad es perfecto, y que debe existir un planeamiento de contingencia para recuperarse ante el desastre. |

**3. Realizar una lectura comprensiva del artículo *“***[***Apagón informático en AFIP***](https://www.iprofesional.com/impuestos/277534-afip-cuil-cuit-Apagon-informatico-en-AFIP-que-servicios-no-funcionaran-hoy)***”*. Luego:**

**a) Analizar los aspectos del “management responsable de SI”.**

* **Punto de vista organizacional:**
  + Debido a la falta de insumos, normas para el trabajo, y desmotivación de los empleados se pueden ver comprometidos los sistemas, por lo que no hay seguridad desde el punto de vista organizacional. O sea que, a nivel técnico, la falta de recursos y procedimientos por parte de los empleados o del equipo de seguridad podría provocar un falla en la seguridad.
* **Punto de vista social:**
  + Desde AEFIP señalaron que “no hay reglas claras de trabajo”, por lo que el sistema no es seguro desde este punto de vista.
  + No es ético que las personas que son responsables de resguardar la información sensible, y de ofrecer los servicios que brinda el sistema, lo utilicen para fines personales (mejoras salariales en definitiva). Aún más, son los contribuyentes los principales afectados de su reclamo gremial, los cuales a través de sus impuestos pagan los sueldos de estos empleados, como también por el desarrollo y mantenimiento del sistema.
* **Punto de vista judicial:**
  + Como la medida se enmarca dentro del derecho de huelga, y hasta el momento no se han filtrado datos personales (que podría violar la ley 25326), puede considerarse que el sistema es seguro desde el punto de vista judicial.
  + Habría que considerar la legalidad desde el punto de vista si los empleados (en ejercicio de su derecho a huelga) pueden disponer de bienes del Estado para hacer su reclamo, y más aún tener el acceso y el poder para disponer de un servicio que maneja información muy sensible.
  + Habría que evaluar la legalidad de las huelgas abusivas como las asambleas, a reglamento y con atención restringida. Evaluando cómo afecta esto la seguridad del sistema.

**b) 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.**

|  |  |
| --- | --- |
| **Management de la seguridad de los IS** | |
| Etapa 1 : | IDENTIFICACIÓN DE RIESGO |

* **Activos:**
  + Hardware de los servidores
  + PCs y estaciones de trabajo
  + Infraestructura de comunicación
  + Software del sistema de Clave Fiscal
  + Software de uso interno en la Afip
  + Datos personales y fiscales de los contribuyentes
* **Vulnerabilidades:**
  + Falta de reglas claras de trabajo, que podrían incluir buenas prácticas, guías, o procedimientos que deban ser seguidos por los empleados o el equipo de seguridad del la AFIP.
  + Falta de insumos básicos para el trabajo diario, dependiendo de lo que incluya esto podría ir desde falta de licencias de SW (antivirus, SO, ofimática, etc.) hasta recursos para pruebas o auditoría para que el equipo de seguridad pueda realizar el management de riesgo adecuadamente.
  + Uso de software pirata debido al problema anterior, que pondría en riesgo la seguridad.
  + Medios y el acceso que permiten a los empleados poder dar de baja todo el sistema de la AFIP.
  + Falta de medios de recuperación que permitan a la Gerencia disponer la replicación de los sistemas en caso de que un evento catastrófico afecte el sistema principal.
* **Amenazas:**

|  |  |  |
| --- | --- | --- |
| **Amenaza** | **Tipo** | **Ataque** |
| Empleado infiel o disconforme que roba dispositivos de HW o SW | Física, Deliberada | Activo |
| Acceso no autorizado al sistema | Física-Lógica, Deliberada | Activo |
| Sabotaje: Medios que permitan a los empleados el cesar de las funciones del sistema de la AFIP | Lógica, Deliberada | Activo |
| Inexistencia de reglas o procedimientos de seguridad por parte de los empleados o del equipo de seguridad | Lógica, Accidental | Pasivo |
| Inexistencia de insumos básicos que permita hacer un management de riesgo o que exponga la seguridad del sistema al no contar con los mismos. | Lógica, Accidental | Pasivo |
| Ciberespionaje | Lógica, Deliberada | Pasivo |

* **Riesgos:**

|  |  |  |
| --- | --- | --- |
| **Riesgos identificados limitados al escenario (artículo)** | | |
|  | **Deliberado** | **Accidental** |
| **Físicos** | Probabilidad de que un empleado disconforme robe un elemento HW o SW | Probabilidad de que la falta de insumos o procedimientos para los empleados o el equipo de seguridad provoque una falla en la seguridad dejando expuestos los sistemas en disponibilidad, confidencialidad o integridad.  Probabilidad de que un acceso no autorizado de los empleados afecte a las funciones del sistema, accidentalmente o por curiosidad. |
|
| **Lógicos** | Probabilidad de que ocurra un sabotaje por parte de los empleados en los sistemas al existir accesos no autorizados y los medios para finalizar la operación de los mismos.  Probabilidad de que ocurra un ciberespionaje por parte de los empleados al existir accesos no autorizados y los medios para finalizar la operación de los mismos. | - |
|

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

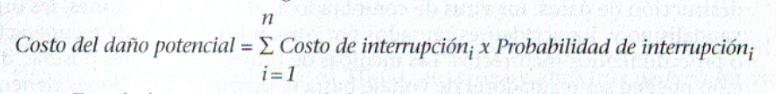
|  |  |
| --- | --- |
| **Management de la seguridad de los IS** | |
| Etapa 2 : | ANÁLISIS DEL RIESGO |

|  |  |  |  |
| --- | --- | --- | --- |
| **Elementos Amenazados** | | | |
| **Equipamiento bajo riesgo en la AFIP** | | | |
| **Recurso** | **Cantidad** | **Valor unitario** | **Valor Total** |
| Datacenter:   * Dell Poweredge R740 Dual Xeon 4110 256gb 8x10tb Server 80tb   ***(Licitación Pública Internacional 47/02)*** | 10 | $1.663.244 | $16.632.440 |
| Infraestructura de comunicación:   * AP: Ubiquiti Uap Ac Lr * Routers: Ubiquiti Er-8 * Switch: Ubiquiti Us-48 * Etc. | 200, 30 y 30 respectivamente | $9000, $30000 y $72000 respectivamente | $1.800.000, $900.000 y $2.016.000 respectivamente |
| Estaciones de trabajo:   * Cuenta con 23000 empleados (datos de 2015) * El 30% requiere estaciones de trabajo   ***(Suposiciones muy conservadoras, simplemente para poner ejemplos)*** | 6900 | $18000 | $124.200.000 |
| TOTAL |  |  | $145.548.440 |

|  |  |  |  |
| --- | --- | --- | --- |
| **Elementos Amenazados** | | | |
| **Informacion bajo riesgo en la AFIP** | | | |
| **Recurso** | **Cantidad** | **Valor unitario** | **Valor Total** |
| Software del sistema de Clave Fiscal | 1  (cantidad de servicios muy grande) | $70.000.000 | $70.000.000 |
| Datos personales y fiscales de los contribuyentes | 450.000 filtraciones  (si existiera tan filtración de los contribuyentes) | $250.000  (Por sentencias a favor de los contribuyentes por daños y perjuicios) | $112.500.000.000‬ |
| Software de uso interno en la Afip | 1 | $30.000.000 | $30.000.000 |
| SW de estaciones de trabajo:  OS: Windows 10  Ofimática: Office 365 | 6900 licencias para cada uno | $8000 por el par W10 + Office | $55.200.000 |
| Falta de información: por fuerza laboral interrumpida y estar el sistema apagado | Por cada 30 min  (dicha cantidad depende de la cantidad de hs de las medidas gremiales) | $400.000  + Cuánto deja de recaudar el Estado  + Fuerza laboral pérdida + Retrasos en otras áreas que esperan información, etc. | $400.000  (depende de la cantidad de hs que el sistema esté apagado). |
| Total |  |  | $112.555.600.000 |

**Análisis de impacto potencial:**

A continuación se analizará el **Costo de daño potencial** según el **costo de interrupción (i)** y la **probabilidad de interrupción (i)**. Esto se hará para cada riesgo identificado.



|  |  |
| --- | --- |
| **Variable** | **Significado** |
| Costo del daño potencial | Es el monto de pérdida al materializarse los riesgos |
| Costo de interrupción **(i)** | Es pérdida potencial de un elemento (activos) evaluado. **(i)**  Fue calculada según los elementos en riesgo según: información, dispositivos, RRHH, definidos en el punto anterior. |
| Probabilidad de Interrupción **(i)** | Es una estimación que permite estimar la frecuencia de ocurrencia de cualquier falla de seguridad, a través del producto entre la probabilidad de agresión por la probabilidad de que la misma tenga éxito.  Se utilizará el siguiente rango de probabilidades:  **Baja = 0% - 30%**  **Media = 31% - 60%**  **Alta = 61% - 100%** |
| Donde **(i)** es un evento probable. Es un riesgo particular identificado.  Y **n e**s el número de eventos. Es la cantidad de amenazas identificadas. | |
|

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Amenaza Particular (i)** | **Probabilidad de agresión** | | **Probabilidad de éxito de la agresión** | | **Probabilidad de Interrupción(i)** | **Costo de interrupción (i)** | **Costo del daño potencial** |
| Error de empleados o del equipo de seguridad por falta de normas o insumos, que provoca una falla de seguridad afectando la disponibilidad, integridad o confiabilidad de la misma.  (afecta elementos de información para el ejemplo) | BAJA | 15% | MEDIA | 40% | 6% | Información  $112.555.600.000 | $6.753.336.000‬‬ |
| Sabotaje  (afecta elementos de información + HW → aire acondicionado o energía del datacenter) | MEDIA | 31% | MEDIA | 31% | 10% | Datacenter  $16.632.440  Información  $112.555.600.000 | $11.257.223.244 |
| Acceso no autorizado  que provoca un accidente en las funciones del sistema, generando una falla de seguridad afectando la disponibilidad, integridad o confidencialidad | BAJA | 10% | MEDIA | 40% | 4% | Información  $112.555.600.000 | $4.502.224.000‬ |
| Ciberespionaje:  falla de seguridad afectando la confidencialidad | BAJA | 30% | BAJA | 20% | 6% | Información  $112.555.600.000 | $6.753.336.000‬ |
| Robo de un elemento HW o SW. | BAJA | 10% | MEDIA | 80% | 8% | HW PC + AP robados = $27000 | $2160 |

**d) Identificar consecuencias primarias y secundarias de la falla de seguridad planteada.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Riesgo** | **Pérdida potencial por falla de seguridad** | **Consecuencias primarias** | **Consecuencias secundarias** |
| Error de empleados o del equipo de seguridad por falta de normas o insumos, que provoque una falla de seguridad afectando la disponibilidad e integridad. | Interrupción del procesamiento a corto o largo plazo.  (Disponibilidad, integridad y  confidencialidad) | * Pérdida en la recaudación * Demandas Millonarias | * Desmotivación de los empleados. * Retraso de entregas de trabajos pendientes. * Otras áreas dependientes de estas entregas son incapaces de realizar su trabajo. * Pérdida de confianza del contribuyente al enterarse de la noticia. * Incomunicación. * Información Gerencial inútil, imprecisa o desactualizada. * Pérdida del nombre de la Institución y su propósito. |
| Sabotaje | Interrupción del procesamiento a corto o largo plazo.  (Disponibilidad e integridad)  Depende del alcance de la Recuperación ante desastres, si existe. | Pérdida en la recaudación. | * Otras áreas dependientes de estas entregas son incapaces de realizar su trabajo. * Retraso de entregas de trabajos pendientes. * Pérdida de confianza del contribuyente al enterarse de la noticia. * Incomunicación. |
| Ciberespionaje | Sanciones por inclumplimieto de obligaciones legales.  (Confidencialidad) | Demandas Millonarias | * Incapacidad de seguir con el negocio. * Pérdida de confianza del contribuyente. * Pérdida del nombre de la empresa |
| Robo de un elemento HW o SW | Revelación de datos confidenciales sobre el manejo interno.  (Confidencialidad) | Datos sensibles internos o de procedimientos de la AFIP | * Retraso de entregas de trabajos pendientes. * Otras áreas dependientes de estas entregas son incapaces de realizar su trabajo. * Incomunicación. |

**e) Qué estrategia de manejo del riesgo propondría utilizar? Con qué esquema de seguridad?**

|  |
| --- |
| **Estrategias de manejo:** |
| **• Prevenir (PR)** |
| **• Reducir (RE)** |
| **• Asumir (AS)** |
| **• Transferir (TR)** |

|  |  |  |
| --- | --- | --- |
| **Línea de Defensa** | **Contramedidas** | **Riesgo** |
| 1 PREVENCIÓN | * Concientización y capacitación sobre la importancia de la seguridad y el seguimiento de las políticas de seguridad. (PR) * Control interno sobre políticas de seguridad, guías, procedimientos, buenas prácticas, etc. (PR) * Optimizar el gasto en seguridad según los niveles de control a los elementos de IS considerando las prioridades en las posibles pérdidas. (PR) * Control de acceso al personal clave a terminales o áreas sensibles. (PR) * Cifrado de comunicaciones e información sensible de los contribuyentes. (PR-RE) * Firewall en infraestructura clave (Datacenter-Dependencias-agencias) de la AFIP. | Error de empleados o del equipo de seguridad por falta de normas o insumos, que provoque una falla de seguridad afectando la disponibilidad, integridad o confiabilidad.  Sabotaje  Ciberespionaje  Robo de un elemento HW o SW |
| 2 DETECCIÓN | * Registro e identificación de dispositivos en áreas clave de la AFIP. (PR) * Antivirus en estaciones de trabajo. * Efectuar el monitoreo de sistemas sobre cuentas y accesos. (PR) * Someter al sistema a pruebas de penetración. (PR) * Implementar soluciones DLP (data loss prevention) para la deteccion y prevencion de datos. (PR) * Videovigilancia en accesos clave y en áreas críticas. (PR-RE) |
| 3 RECUPERACIÓN |
| * Backup y cifrado diario de la información sensible (PR-RE) * Datacenter de respaldo en caso de catástrofe. * Protocolos de seguridad sobre recuperación ante desastre. (PR-RE) * Entrenamiento y Simulaciones al personal sobre la recuperación ante el desastre en sus diferentes grados(PR-RE) |

**f) ¿Qué políticas de seguridad recomendaría?**

**Propósito:** Implementar controles de acceso físicos y lógicos en sus redes, sistemas de TI y servicios para proporcionar acceso de usuario autorizado, granular, auditable y apropiado, y para garantizar preservación adecuada de la confidencialidad, integridad y disponibilidad de los datos de acuerdo con la Política de seguridad de la información.

**Alcance:** Esta política cubre todas las redes de la AFIP, salas de comunicaciones, sistemas de TI, datos y usuarios autorizados.

**Cuentas privilegiadas:** La asignación de derechos de privilegio (por ejemplo, administrador local, administrador de dominio, superuser, acceso root) estará restringida y controlada por el área de IS y no se proporcionará por defecto.

**Métodos de control de acceso:** El acceso a los datos se controla de manera variada y adecuada de acuerdo con los niveles de clasificación de datos descritos en la Política de seguridad de la información de la AFIP.

Los métodos de control de acceso utilizados por defecto incluyen:

* Inicio de sesión explícito en dispositivos,
* Windows: permisos de acceso a archivos y carpetas,
* Limitaciones de privilegios de cuenta de usuario,
* Derechos de acceso al servidor y estación de trabajo,
* Permisos de firewall,
* Derechos de autenticación IIS / Apache intranet / extranet,
* Derechos de inicio de sesión de usuario AFIP,
* Derechos de acceso a la base de datos y ACL,
* Cifrado en reposo y en vuelo.

El control de acceso se aplica a todas las redes, servidores, estaciones de trabajo, computadoras portátiles y dispositivos móviles propiedad de AFIP, y servicios ejecutados en nombre de AFIP.

**Pruebas de penetración:** La provisión de control de acceso de la AFIP se somete regularmente a pruebas de penetración para determinar la efectividad de los controles existentes y exponer cualquier debilidad. Las pruebas serán donde sea apropiado y acordado.

**Pautas para el uso de cuentas:** Se espera que los usuarios se familiaricen y cumplan con las políticas, estándares y pautas de la AFIP para un uso apropiado y aceptable de las redes y sistemas. Esto incluye las condiciones de Uso de los servicios de TI de la AFIP y la política de uso aceptable.

**Acceso a información confidencial, restringida y de uso interno:** El acceso a la información "confidencial", "restringida" y "de uso interno" se limitará a la autorización de personas cuyas responsabilidades laborales o de estudio lo requieran, según lo determine la ley, o el acuerdo contractual con partes interesadas.

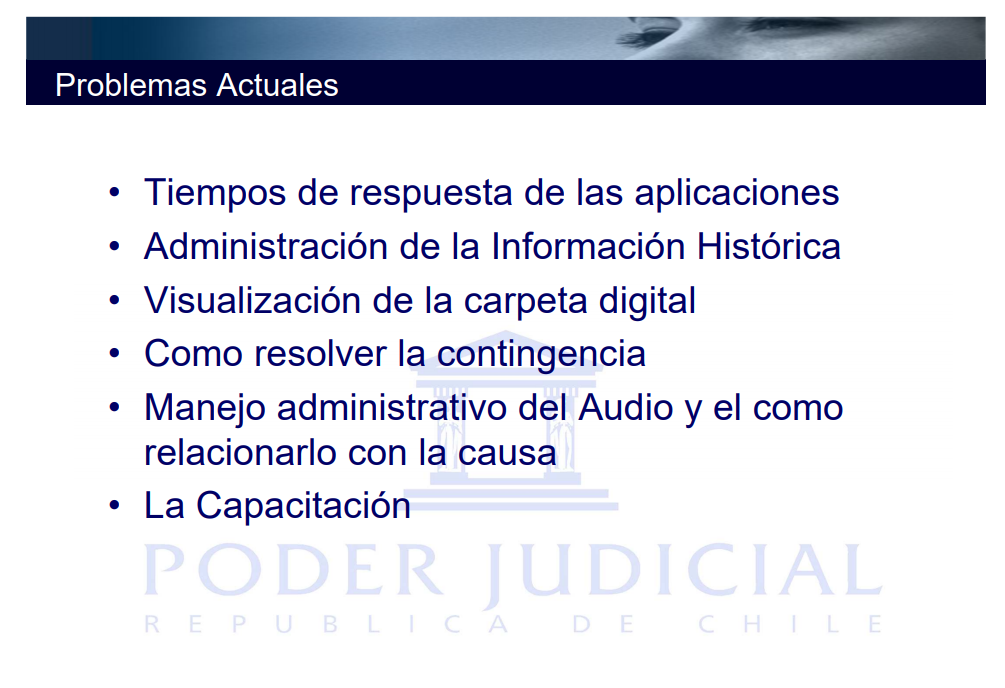
**Transparencia y Información**: AFIP proporcionará a todos los empleados, terceros contratados, proveedores el acceso in situ a la información que necesitan para llevar a cabo sus responsabilidades de manera tan efectiva y eficiente como posible.

**Aplicación:** Cualquier empleado que por sus tareas o funciones establecidas, haya violado las políticas de seguridad vigentes, por acción u omisión, estará sujeto a medidas disciplinarias que pueden incluir terminación del empleo.

**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”*).**

|  |  |
| --- | --- |
| **Management de la seguridad de los IS** | |
| Etapa 1 : | IDENTIFICACIÓN DE RIESGO |

* **Activos:**
  + Hardware de los servidores
  + PCs y estaciones de trabajo
  + Infraestructura de comunicación
  + Software de uso interno del PJUD
  + Software para ofrecer servicios externos del PJUD (abogados, peritos, acusados, fiscales, etc.)
  + Información de causas, sentencias y demás documentación relevante para el PJUD
  + Datos personales y de las causas en curso o con sentencia que por su sensibilidad no pueden estar disponibles al público general (informantes, arrepentidos, bajo protección, etc.)
* **Vulnerabilidades:**
  + Empleado desleal que puede revelar información sensible de las causas.
  + Evento catastrófico sobre la infraestructura del PJUD (terremoto, tsunami, inundación, volcán)
  + Falla en la seguridad que pudiera ser usada para filtrar datos sensibles
  + Error en la configuración del SW de los equipos por parte de los empleados, que deja una brecha de seguridad
  + Falta de medios de recuperación que permitan al PJUD disponer la replicación de los sistemas en caso de que un evento catastrófico afecte al sistema principal
  + Nuevos virus, ransomware o malware que afecten a los sistemas del PJUD.

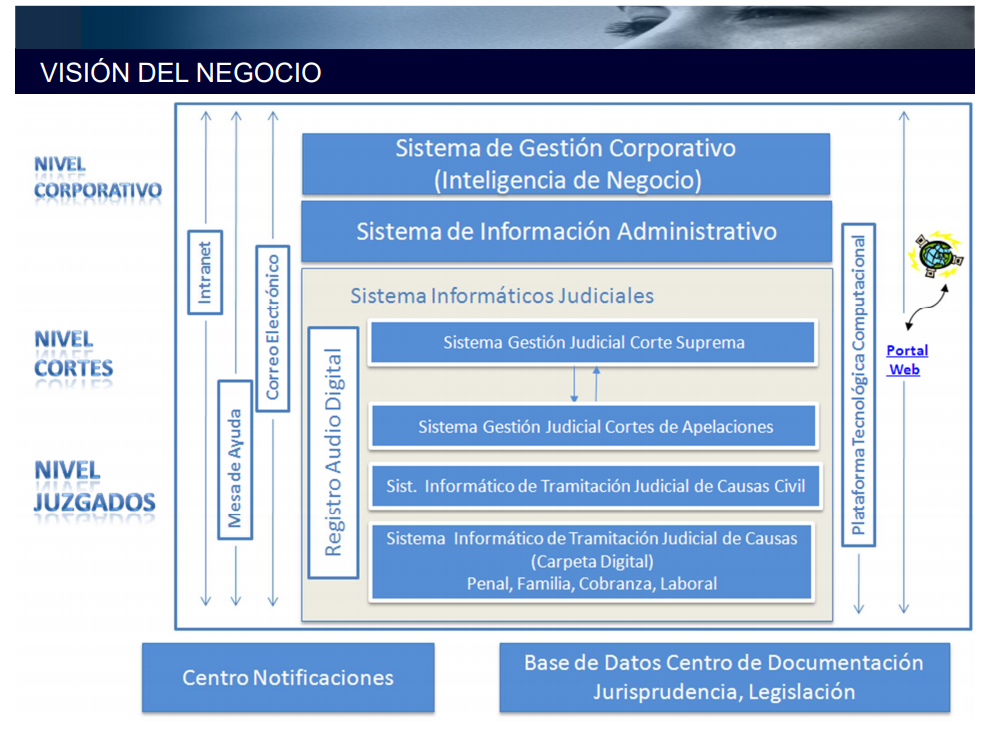


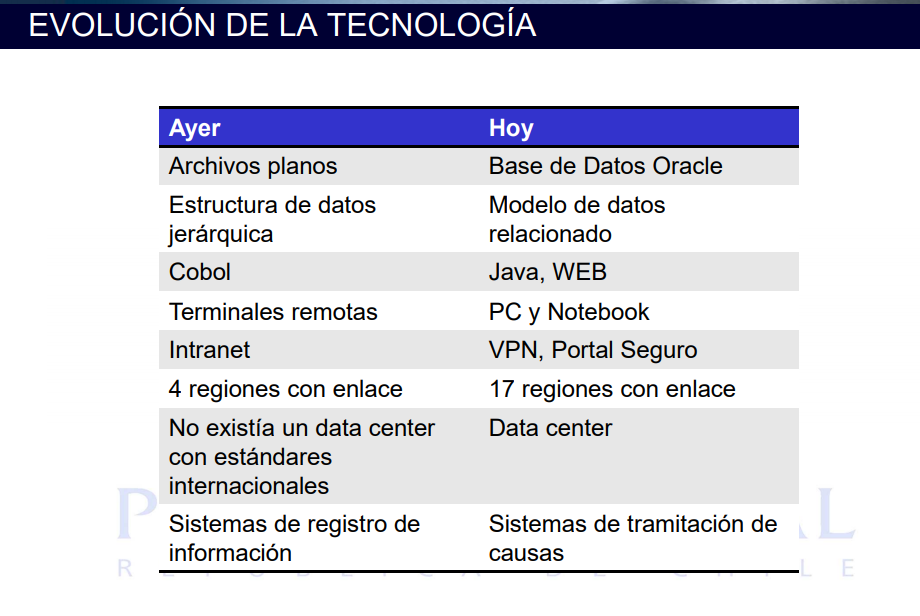
|  |  |  |
| --- | --- | --- |
| **Amenaza** | **Tipo** | **Ataque** |
| Errores en la configuración en el  SW o HW de los equipos por los empleados | Física-Lógica, Accidental | Activo |
| Evento catastrófico que afecte a la infraestructura de IS del PJUD | Física, Accidental | - |
| Sabotaje que afecte a la información o infraestructura sensible del PJUD | Física-lógica, Deliberada | Activo |
| Espionaje que afecte a la información sensible del PJUD | Física, Deliberada | Pasivo |
| Ciberespionaje que afecte a la información del PJUD | Lógica, Deliberada | Pasivo |
| Virus, Ransomware, Malware | Lógica, Deliberada | Activo |

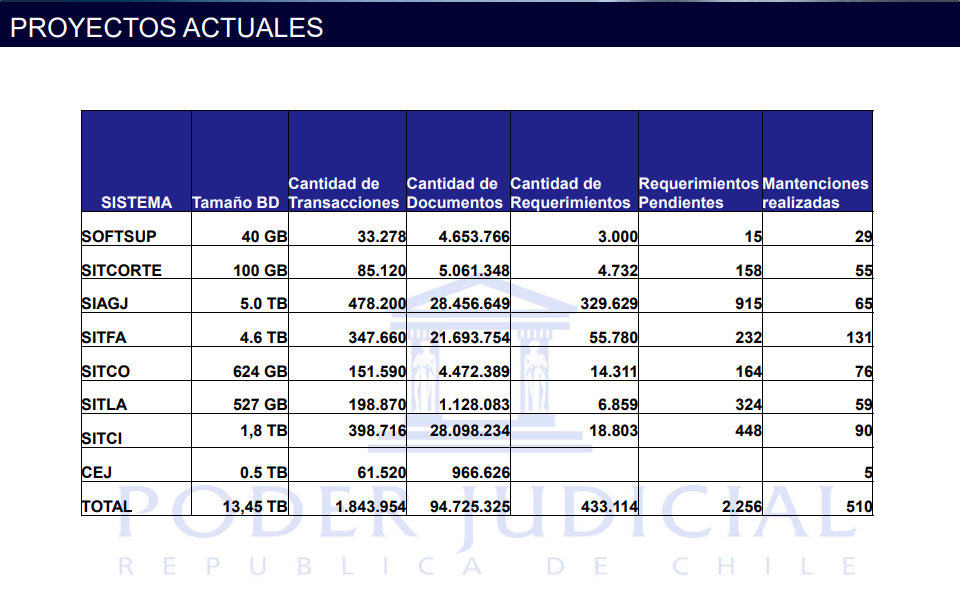
* **Riesgos:**

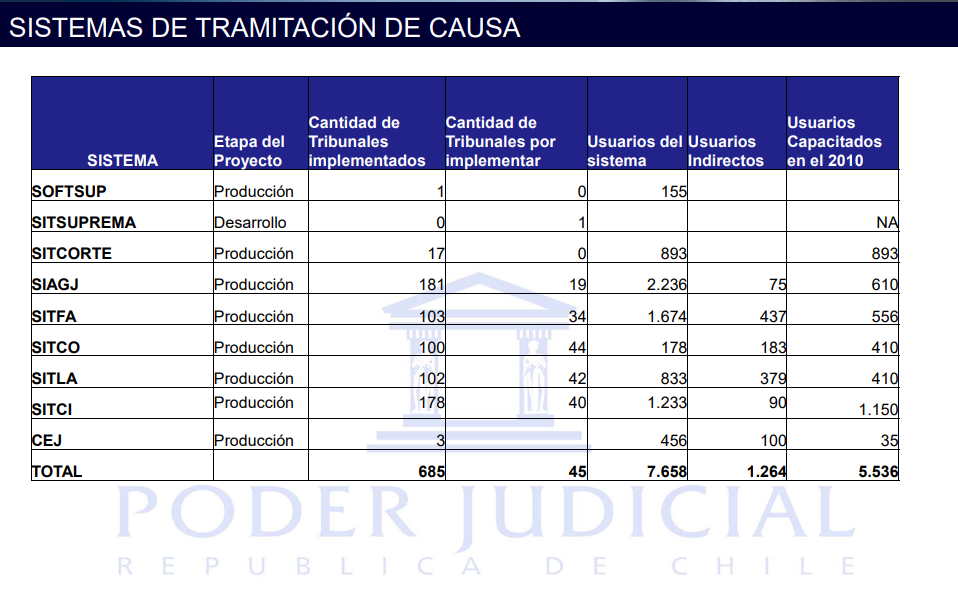
|  |  |  |
| --- | --- | --- |
| **Riesgos identificados para el PJUD** | | |
|  | **Deliberado** | **Accidental** |
| **Físicos** | Probabilidad de que un empleado desleal esté espiando información sensible del PJUD. | Probabilidad de que un evento catastrófico afecte a la infraestructura de IS de PJUD. |
|
| **Lógicos** | Probabilidad de que los sistemas estén bajo ciberespionaje comprometiendo la información del PJUD.  Probabilidad de que un empleado o agente externo provoque un sabotaje que afecte a la información o infraestructura sensible del PJUD.  Probabilidad de que se genere una infección de virus, Ransomware, malware, etc., que comprometa la información del PJUD. | Probabilidad de que un empleado cometa errores en la configuración en el SW o HW de los equipos, comprometiendo información sensible del PJUD. |
|
|

|  |  |
| --- | --- |
| **Management de la seguridad de los IS** | |
| Etapa 2 : | ANÁLISIS DEL RIESGO |

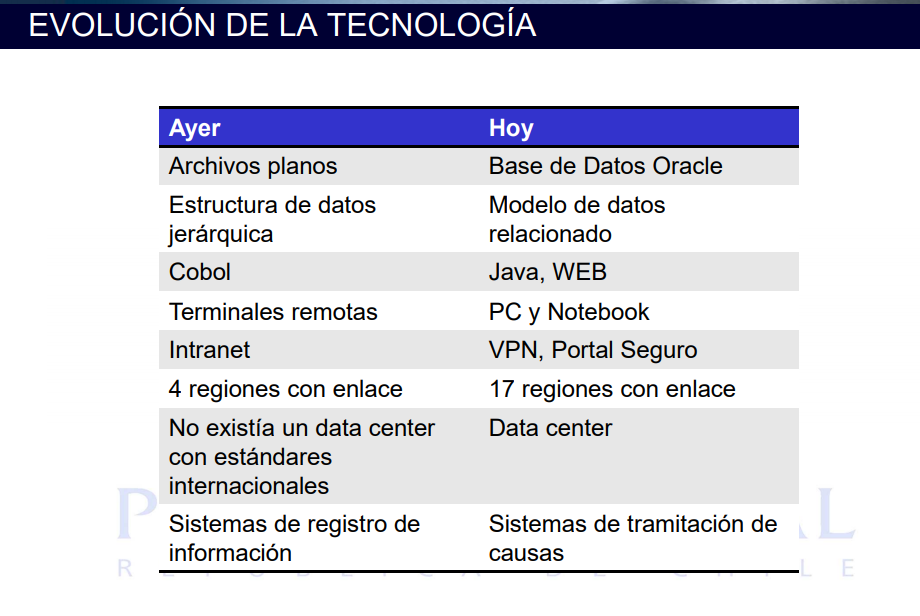


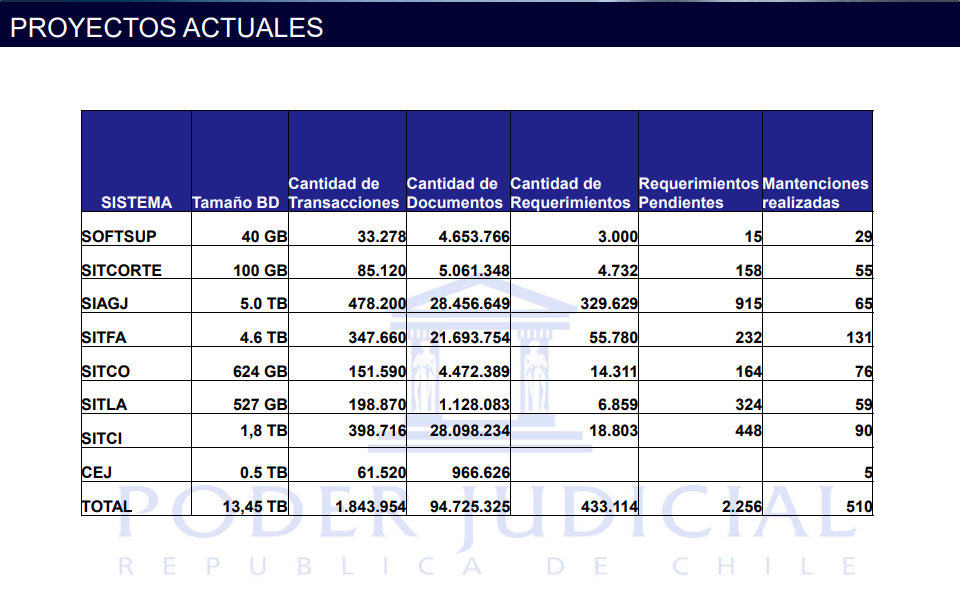
****

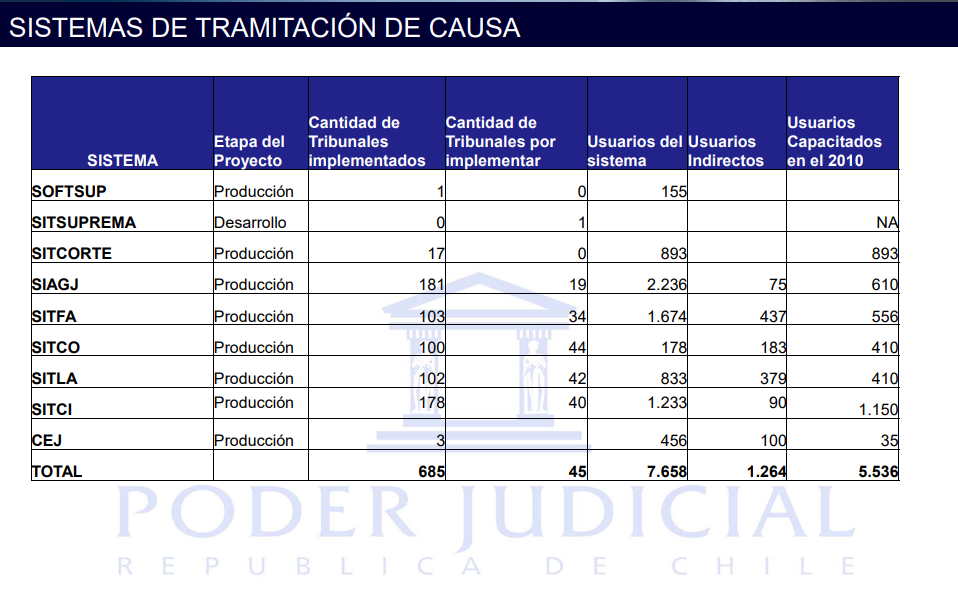




|  |  |  |  |
| --- | --- | --- | --- |
| **Elementos Amenazados** | | | |
| **Equipamiento bajo riesgo en el PJUD** | | | |
| **Recurso** | **Cantidad** | **Valor unitario** | **Valor Total** |
| Datacenter:  Dell PowerEdge R630 Server Bundle Including - Intel Xeon E5-2620 v4 8-Core 2.1GHz CPU, 32GB DDR4 RAM, 4TB SSD  Incluye las condiciones necesarias en seguridad física, virtual, eléctrica y ambiental requeridas por el equipo. | 10 | $320.000 | $3.200.000‬ |
| Infraestructura de comunicación:   * AP: Ubiquiti Uap Ac Lr * Routers: Ubiquiti Er-8 * Switch: Ubiquiti Us-48 * Ubiquiti Airfiber 11FX * Ubiquiti Litebeam M5 * Etc. | 55, 30, 30, 7 y 10, respectivamente | $9000, $30000, $72000, $100000 y $10000, respectivamente | $4.355.000 |
| Estaciones de trabajo:   * Al 27 de junio de 2018 12235 personas integran el Poder Judicial. * Con 18.044‬ estaciones de trabajo * Más 1.924 Notebooks   ***(Suposiciones muy simplistas y conservadoras, simplemente para poner ejemplos)*** | 18.044‬  1.924 | $18.000  $25.000 | $223.555.000  $48.100.000 |
| TOTAL |  |  | $231.839.000‬ |

****

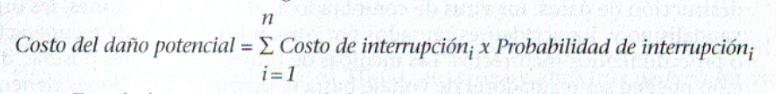




|  |  |  |  |
| --- | --- | --- | --- |
| **Elementos Amenazados** | | | |
| **Informacion bajo riesgo en el PJUD** | | | |
| **Recurso** | **Cantidad** | **Valor unitario** | **Valor Total** |
| Software de uso externo | Portal Web del Poder Judicial de Chile  (cantidad muy grande de servicios) | $10.000.000 | $10.000.000 |
| Información sensible: Datos personales, patrimoniales o de causas sensibles.  Por ejemplo, la OJV (Oficina Judicial Virtual) diariamente tiene un ingreso de 50.000 escritos y 400.000 documentos. Además, el Portal Web del PJUD tiene más de 4 millones de solicitudes. Mucho de esto es material sensible. | 10.000 filtraciones  (si existiera tan sólo una pequeña filtración de los datos de causas sensibles o de datos personales) | $250.000  (Por sentencias a favor de los afectados por daños y perjuicios + posible pérdida de vidas) | $2.500.000.000‬ |
| Software de uso interno del PJUD | +17 | - | $10.000.000 |
| SW de estaciones de trabajo:  OS: Windows 10  Ofimática: Office 365 | 12000 licencias para cada uno | $8000 por el par W10 + Office | $96.000.000 |
| Falta de información: por fuerza laboral interrumpida al estar el sistema apagado o con funcionalidad limitado o bajo ataque. | x hs | $200.000  + Horas extra de re-trabajo  + Fuerza laboral perdida  + Retrasos en otras áreas que esperan información, etc. | $200.000  (depende de la cantidad de hs que el sistema esté apagado o limitado). |
| Total |  |  | $2.606.200.000 |

**Análisis de impacto potencial:**

A continuación se analizará el **Costo de daño potencial** según el **costo de interrupción (i)** y la **probabilidad de interrupción (i)**. Esto se hará para cada riesgo identificado.



|  |  |
| --- | --- |
| **Variable** | **Significado** |
| Costo del daño potencial | Es el monto de pérdida al materializarse los riesgos |
| Costo de interrupción **(i)** | Es la pérdida potencial de un elemento (activo) evaluado. **(i)**  Fue calculada según los elementos en riesgo, según: información, dispositivos y RRHH, definidos en el punto anterior. |
| Probabilidad de Interrupción **(i)** | Es una estimación que permite estimar la frecuencia de ocurrencia de cualquier falla de seguridad, a través del producto entre la probabilidad de agresión por la probabilidad de que la misma tenga éxito.  Se utilizará el siguiente rango de probabilidades:  **Baja = 0% - 30%**  **Media = 31% - 60%**  **Alta = 61% - 100%** |
| Donde **(i)** es un evento probable. Es un riesgo particular identificado.  Y **n e**s el número de eventos. Es la cantidad de amenazas identificadas. | |
|

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Amenaza Particular (i)** | **Probabilidad de agresión** | | **Probabilidad de éxito de la agresión** | | **Probabilidad de Interrupción(i)** | **Costo de interrupción (i)** | **Costo esperado** |
| Empleado que comete **errores en la configuración** en el SW o HW de los equipos, comprometiendo información sensible del PJUD.  (afecta elementos de información para el ejemplo) | BAJA | 5% | MEDIA | 60% | 3% | Información  $2.606.200.000 | $78.186.000‬ |
| **Evento catastrófico** (tsunami-terremoto) que afecte a la infraestructura de IS de PJUD.  (afecta elementos de información (integridad) + data center para el ejemplo) | BAJA | 5% | ALTA | 90% | 4,5% | Información  $2.606.200.000  Datacenter  $3.200.000‬  \*Más el costo de las horas con el sistema sin ofrecer servicio. | $117.423.000  \*sin backup o respaldo de la información el daño sería catastrófico‬ |
| **Ciberespionaje:** Los sistemas están siendo espiados comprometiendo la información del PJUD.  (afecta elementos de información para el ejemplo) | MEDIA | 60% | BAJA | 5% | 3% | Información  $2.500.000.000 | $75.000.000‬ |
| Empleado o agente externo que provoque un **sabotaje** que afecte a la información o infraestructura sensible del PJUD.  (afecta elementos como el datacenter corte de energía-incendio provocados para el ejemplo) | BAJA | 5% | MEDIA | 50% | 2.5% | Información  $2.500.000.000 | $62.500.000‬ |
| **Infección** de virus, Ransomware, malware, etc., que comprometa la información del PJUD. | ALTA | 80% | BAJA | 5% | 3% | Información  $2.500.000.000  \*Más el costo de las horas con el sistema sin ofrecer servicio. | $75.000.000‬ |
| **Espionaje**:Empleado desleal que esté espiando información sensible del PJUD. | BAJA | 5% | BAJA | 30% | 3% | Información  $2.500.000.000 | $75.000.000‬ |

**Consecuencias**

|  |  |  |  |
| --- | --- | --- | --- |
| **Riesgo** | **Pérdida potencial por falla de seguridad** | **Consecuencias primarias** | **Consecuencias secundarias** |
| Empleado que comete **errores en la configuración** en el SW o HW de los equipos, comprometiendo información sensible del PJUD. | Depende del error:  Interrupción del procesamiento a corto o largo plazo.  Brecha de seguridad afectado la información en su disponibilidad, integridad o confidencialidad | Pérdida parcial o total en el ofrecimiento de los servicios de justicia.  Demandas Millonarias | * Desmotivación de los empleados. * Retraso de entregas de trabajos pendientes. * Otras áreas dependientes de estas entregas son incapaces de realizar su trabajo. * Pérdida de confianza de las personas en proceso al enterarse de la noticia. * Incomunicación. * Información Gerencial inútil, imprecisa o desactualizada. * Pérdida del nombre de la Institución |
| **Evento catastrófico** (tsunami-terremoto) que afecte a la infraestructura de IS de PJUD. | Interrupción del procesamiento a corto o largo plazo.  (Disponibilidad e integridad)  Depende del alcance de la Recuperación ante desastres, si existe. | Colapso de los servicios de Justicia  Depende del alcance de la Recuperación ante él desastres, si existe. | * Otras áreas dependientes de estas entregas son incapaces de realizar su trabajo. * Retraso de entregas de trabajos pendientes. * Pérdida de confianza de las personas al enterarse de la noticia. * Incomunicación. * Desmotivación de los empleados. |
| **Ciberespionaje:** Los sistemas están siendo espiados comprometiendo la información del PJUD. | Sanciones por inclumplimieto de obligaciones legales.  (Confidencialidad)  Revelación de datos confidenciales sobre el manejo interno de PJUD  (Confidencialidad) | Demandas Millonarias  Filtración de datos sensibles internos o de procedimientos del PJUD | * Incapacidad de seguir con las actividades judiciales hasta solucionar la fuga de información. * Pérdida de confianza del pueblo en el Poder Judicial. * Pérdida del nombre de la Institución |
| Empleado o agente externo que provoque un **sabotaje** que afecte a la información o infraestructura sensible del PJUD. | Interrupción del procesamiento a corto o largo plazo.  (Disponibilidad e integridad)  Depende del alcance de la Recuperación ante desastres, si existe. | Daños a la infraestructura, integridad o disponibilidad de la información | * Retraso de entregas de trabajos pendientes. * Otras áreas dependientes de estas entregas son incapaces de realizar su trabajo. * Incomunicación. |
| **Espionaje**: Empleado desleal que esté espiando información sensible del PJUD. | Revelación de datos confidenciales sobre el manejo interno del PJUD  (Confidencialidad) | Filtración de datos sensibles internos o de procedimientos del PJUD  Demandas Millonarias | * Problemas al realizar las actividades judiciales hasta solucionar la fuga de información. * Pérdida de confianza del pueblo en el Poder Judicial. * Pérdida del nombre de la Institución |
| **Infección** de virus, Ransomware, malware, etc., que comprometa la información del PJUD. | Interrupción del procesamiento a corto o largo plazo.  (Disponibilidad e integridad)  Revelación de datos confidenciales sobre el manejo interno del PJUD  (Confidencialidad)  Depende del alcance de la Recuperación ante desastres, si existe. | Pérdida parcial o total en el ofrecimiento de los servicios de justicia  Filtración de datos sensibles internos o de procedimientos del PJUD  Demandas Millonarias | * Problemas al realizar las actividades judiciales hasta solucionar la infección de información. * Pérdida de confianza del pueblo en el Poder Judicial. * Pérdida del nombre de la Institución * Retraso de entregas de trabajos pendientes. * Otras áreas dependientes de estas entregas son incapaces de realizar su trabajo * Información Gerencial inútil, imprecisa o desactualizada. * Incomunicación. |

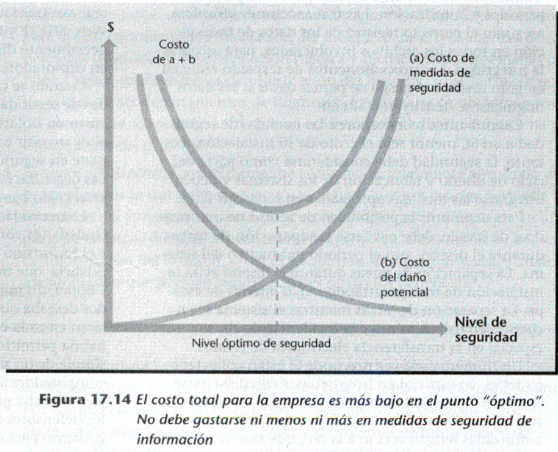
|  |  |
| --- | --- |
| **Management de la seguridad de los IS** | |
| Etapa 3: | MANEJO DE RIESGO |

**Estrategias y seguridad para las líneas de defensa del PJUD:**

|  |
| --- |
| **Estrategias de manejo:** |
| **• Prevenir (PR)** |
| **• Reducir (RE)** |
| **• Asumir (AS)** |
| **• Transferir (TR)** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Línea de Defensa** | **Controles y Contramedidas** | **Costo**  **Contramedidas** | **Riesgo más importantes**  **considerados** |
| 1 PREVENCIÓN | * Concientización y capacitación sobre la importancia de la seguridad y el seguimiento de las políticas de seguridad (PR). | xxxx$ | Sabotaje  **Evento catastrófico** (ej:tsunami-terremoto) que afecte a la infraestructura crítica del PJUD.  Ciberespionaje  Robo de un elemento HW o SW  Error de empleados o del equipo de seguridad por falta de normas o insumos, que provoque una falla de seguridad afectando la disponibilidad, integridad o confiabilidad.  **Infección** de virus, Ransomware, malware, etc., que comprometa la información del PJUD |
| * Control interno sobre el seguimiento de políticas de seguridad, guías, procedimientos, buenas prácticas establecidas, etc. (PR) | xxxx$ |
| * División y asignación de responsabilidades a los empleados en cuanto al el uso de los sistemas y el control de seguridad de los mismos (configuración,implementación, verificación), separación de roles y sin responsables exclusivos de realizar una tarea completamente (control de pares) .(PR) | xxxx$ |
| * Control de acceso al personal clave a terminales o áreas sensibles. (PR) | xxxx$ |
| * Cifrado de comunicaciones e información sensible de los contribuyentes. (PR-RE) | xxxx$ |
| * Firewall en infraestructura clave (Datacenter, Dependencias, agencias) del PJUD. | xxxx$ |
| 2 DETECCIÓN | * Registro e identificación de dispositivos en áreas clave del PJUD. (PR) | xxxx$ |
| * Antivirus en estaciones de trabajo. | xxxx$ |
| * Efectuar el monitoreo de sistemas sobre cuentas y accesos (PR) | xxxx$ |
| * Someter al sistema a pruebas de penetración. (PR) | xxxx$ |
| * Implementar soluciones DLP (data loss prevention) para la deteccion y prevencion de datos (PR) | xxxx$ |
| * Videovigilancia en accesos clave y en áreas críticas (RE-PR) | xxxx$ |
| 3 RECUPERACIÓN |
| * Backup y cifrado diario de la información sensible (PR-RE) | xxxx $ |
| * Datacenter de respaldo en caso de catástrofe. | xxxx $ |
| * Protocolos de seguridad sobre recuperación ante desastres (PR-RE) | xxxx $ |
| * Entrenamiento y Simulaciones al personal sobre la recuperación ante el desastre en sus diferentes grados(PR-RE) | xxxx $ |
|

Hay que recordar que para responder la pregunta de ***¿cuánto debe gastar el PJUD en medidas de seguridad para datos?*** Se deben considerar los costos del daño potencial (calculado antes por cada riesgo identificado) y el costo de instalar y mantener la medida de seguridad (detección, prevención, recuperación). Cuanto más rigurosas sean las medidas de seguridad, más pequeña es la posibilidad de que exista un daño. Esto significa que a medida que aumenta el costo de las medidas de seguridad, disminuye el costo del daño potencial. El PJUD colocará esta inversión en el punto óptimo, o sea, donde el total de ambos costos disminuye.



**POLÍTICAS DE SEGURIDAD**

**CONTROL DE ACCESO**

**Propósito:** Implementar controles de acceso físicos y lógicos en sus redes, sistemas de TI y servicios para proporcionar acceso de usuario autorizado, granular, auditable y apropiado, y para garantizar preservación adecuada de la confidencialidad, integridad y disponibilidad de los datos de acuerdo con la Política de seguridad de la información.

**Alcance:** Esta política cubre todas las redes de la PJUD, salas de comunicaciones, sistemas de TI, datos y usuarios autorizados.

**Cuentas privilegiadas:** La asignación de derechos de privilegio (por ejemplo, administrador local, administrador de dominio, superuser, acceso root) estará restringida y controlada por el área de IS y no se proporcionará por defecto.

**Métodos de control de acceso:** El acceso a los datos se controla de manera variada y adecuada de acuerdo con los niveles de clasificación de datos descritos en la Política de seguridad de la información del PJUD.

Los métodos de control de acceso utilizados por defecto incluyen:

* Inicio de sesión explícito en dispositivos,
* Windows: permisos de acceso a archivos y carpetas,
* Limitaciones de privilegios de cuenta de usuario,
* Derechos de acceso al servidor y estación de trabajo,
* Permisos de firewall,
* Derechos de autenticación IIS / Apache intranet / extranet,
* Derechos de inicio de sesión de usuario PJUD,
* Derechos de acceso a la base de datos y ACL,
* Cifrado en reposo y en vuelo.

El control de acceso se aplica a todas las redes, servidores, estaciones de trabajo, computadoras portátiles y dispositivos móviles propiedad del PJUD, y servicios ejecutados en su nombre.

**Pruebas de penetración:** La provisión de control de acceso en el PJUD se somete regularmente a pruebas de penetración para determinar la efectividad de los controles existentes y exponer cualquier debilidad. Las pruebas serán donde sea apropiado y acordado.

**Pautas para el uso de cuentas:** Se espera que los usuarios se familiaricen y cumplan con las políticas, estándares y pautas de la PJUD para un uso apropiado y aceptable de las redes y sistemas. Esto incluye las condiciones de Uso de los servicios de TI del PJUD y la política de uso aceptable.

**Acceso a información confidencial, restringida y de uso interno:** El acceso a la información "confidencial", "restringida" y "de uso interno" se limitará a la autorización de personas cuyas responsabilidades laborales o de estudio lo requieran, según lo determine la ley, o el acuerdo contractual con partes interesadas.

**Transparencia e Información**: El PJUD proporcionará a todos los empleados, terceros contratados, proveedores el acceso in situ a la información que necesitan para llevar a cabo sus responsabilidades de manera tan efectiva y eficiente como posible.

**Aplicación:** Cualquier empleado que por sus tareas o funciones establecidas, haya violado las políticas de seguridad vigentes, por acción u omisión, estará sujeto a medidas disciplinarias que pueden incluir terminación del empleo.

**Seguridad de las comunicaciones**

**Propósito:** Esta política proporciona un conjunto de procedimientos y estándares para implementar tecnologías inalámbricas dentro del entorno de red. Proporciona a los administradores de red que implementan y administran estas tecnologías un conjunto básico de requisitos que documentan la conectividad, la seguridad y la supervisión del dispositivo.

**Alcance:** Esta política se aplica a todo el personal que diseña, instala y ofrece soporte a redes inalámbricas.

**Autenticación y Transmisión (prohibitiva-Autenticidad):** Todos los puntos de acceso inalámbrico que conectan clientes a la red interna (LAN) requerirán que los usuarios proporcionen autenticación única a través de canales seguros, y todos los datos transmitidos se cifran según la tecnología de encriptación aprobada por el área de seguridad de IS.

**Localización física (prohibitiva-Posesión):** Deben establecerse mecanismos de seguridad para evitar el robo, la alteración o el mal uso de puntos de acceso/estaciones base. Todos los dispositivos deberán estar bloqueados y asegurados de manera adecuada.

**Tecnología aprobada (prohibitiva-Posesión):** Todo terminal, dispositivo o hardware de LAN inalámbrica usado para conectarse a una red deberán ser configurados para usar las últimas actualizaciones de seguridad disponibles.

**Registrar puntos de acceso (prohibitiva-Posesión):** Todos los puntos de acceso inalámbricos/ estaciones base conectados a la red deben estar registrados y aprobados por el área de seguridad de IS. Todos los puntos de acceso/estaciones base aprobados están sujetos a pruebas y auditorías periódicas de penetración.

**Cumplimiento (prohibitiva-Confidencialidad):** Cualquier empleado que por sus tareas o funciones establecidas, haya violado las políticas de seguridad vigentes, por acción u omisión, estará sujeto a medidas disciplinarias que pueden incluir terminación del empleo.

**Gestión de activos**

**Propósito:** El propósito de esta política es proporcionar reglas consistentes para garantizar que las copias de seguridad estén disponibles cuando sea necesario.Esta política de respaldo está estrechamente relacionada con la continuidad del servicio de justicia y la recuperación ante desastres, ya que protege contra eventos que son relativamente probables.

**Alcance:** Todos los datos almacenados en los servidores de archivos, servidores de correo electrónico, servidores de red, servidores web, servidores de bases de datos del PJUD.

Se realizarán copias de seguridad de los firewalls y servidores de acceso remoto. Es responsabilidad del usuario designado garantizar que los datos importantes se trasladen al servidor de archivos.

**Almacenamiento del respaldo:** Cuando se almacene en el sitio, los medios de respaldo deben almacenarse en un contenedor a prueba de fuego en un área de acceso controlado.

Cuando se traslada fuera del sitio, esta lo hará con una escolta de seguridad, hasta una instalación reforzada que utiliza métodos aceptados de controles ambientales, incluida la extinción de incendios y procesos de seguridad para garantizar integridad de todos medios de copia de seguridad.

**Procedimientos de restauración y documentación:** El Máximo responsable del área de información del PJUD y el personal de TI a su cargo son responsables de los datos, los procedimientos de restauración, la elección de la herramienta para realizar el respaldo, determinar quién es responsable de la restauración, cómo se realiza, en qué circunstancias, cuánto tiempo tomará desde la solicitud hasta la restauración y la documentación asociada.

**Retención del respaldo:** El tiempo en retención será establecido de la siguiente forma:

* Las copias de seguridad incrementales deben guardarse durante una semana.
* Las copias de seguridad completas deben guardarse durante un mes.
* Las copias especiales por solicitud se programará según los recursos humanos disponibles en el área de TI y la prioridad del respaldo en cuestión.

**Prueba de restauración:** Las restauraciones de respaldo deben probarse cuando se realiza algún cambio que pueda afectar el sistema de respaldo (herramienta). Las restauraciones de respaldo también deben probarse mensualmente para garantizar la integridad de las copias de seguridad en caso de crisis.

**Duplicación de datos:** Al identificar y clasificar los datos del PJUD, es importante comprender dónde pueden estar esos datos almacenados, particularmente como copias duplicadas, de modo que esta política se pueda aplicar a todos los duplicados de información.

**Requisitos de retención:** Como regla general, los datos operativos de la empresa y los datos del cliente deben conservarse de acuerdo con la Política de respaldo de datos establecida en el PJUD. Los datos personales deben eliminarse o destruirse cuando ya no sean necesarios. Los datos específicos a un determinado proceso judicial pueden conservarse y eliminarse de acuerdo con los requisitos legales vigentes.

**Retención de datos cifrados:** Si alguna información retenida bajo esta política se almacena en un formato cifrado, se debe tener en cuenta el almacenamiento seguro de las claves de cifrado. Éstas deben conservarse siempre que se retengan los datos que descifran.

**Destrucción de datos:** La destrucción de datos es un componente crítico de esta política de retención de datos. Cuando el plazo de retención caduca, la Firma debe destruir activamente los datos cubiertos por esta política. Si el responsable siente que ciertos datos no debe ser destruidos, debe identificarlos y comunicar a su superior para que se evalúe la posibilidad de generar una excepción en la política bajo circunstancias especiales.

**Otros aspectos muy importantes a incorporar en la política de seguridad son :**

* **Procedimientos** para reconocer actividades no autorizadas.
* **Definir acciones** a tomar en caso de **incidentes**.
* **Definir acciones** a tomar cuando se **sospeche de actividades no autorizadas**.
* Conseguir que la **política sea respaldada** por el estamento más alto posible dentro de la organización.
* **Divulgar la política** de forma eficiente entre los usuarios y administradores.
* Articular **medidas de auditoría** de nuestro propio sistema de seguridad.
* Establecer plazos de **revisión de la política** en función de resultados obtenidos.

|  |  |
| --- | --- |
| **Management de la seguridad de los IS** | |
| Etapa 4: | RECUPERACIÓN ANTE EL DESASTRE |

La prevención total del riesgo es poco práctica o imposible. Por lo que se debe planificar cómo enfrentarse a las inevitables rupturas de seguridad y cómo recuperarse de ellas. Esto es lo que se denomina plan de contingencias, e incluye planes y métodos de trabajo que permitan que la empresa sobreviva al desastre, y a los procesos a largo plazo para que la organización se recupere.

|  |  |  |  |
| --- | --- | --- | --- |
| **Descripción** | **Probabilidad** | **Impacto** | **Riesgo** |
| **Errores en la configuración** | BAJA | ALTO | BAJO |
| **Evento catastrófico** | BAJA | EXTREMO | BAJO |
| **Ciberespionaje** | BAJA | ALTO | BAJO |
| **Sabotaje** | BAJA | ALTO | BAJO |
| **Espionaje** | BAJA | ALTO | BAJO |
| **Infección** | BAJA | ALTO | BAJO |

Consideramos que la prioridad más grande que tiene el PJUD en la planificación de contingencias es tener un respaldo de su datacenter y de toda la infraestructura de respaldo asociada. La razón es simple: es clave para ofrecer los servicios de justicia a un país entero. La falta de servicio o “downtime” tiene costos en la imagen, en la productividad, posibles problemas legales (falta de acceso a la justicia), etc. El costo de no resolver cuestiones legales de las personas (más allá de los inmensos costos que conlleva a los contribuyentes), cercena un derecho básico del Estado de derecho, el acceso a la justicia. Sin acceso a la justicia, las personas no pueden hacer oír su voz, ni ejercer sus derechos, hacer frente a la discriminación, etc. Como tal es crítico tener un datacenter de respaldo para poder hacer frente a contingencias producto de una catástrofe en el datacenter actual.

Hay que pensar en el equilibrio de costos y riesgos en este caso, claramente los costos de semejante inversión no son fáciles para cualquier organización, pero el riesgo de no tener ninguna contramedida en caso de catástrofe dejaría a los servicios de justicia ofrecidos por el PJUD prácticamente paralizados, y sin un tiempo razonable de recuperación a la vista. Los riesgos son sencillamente demasiados altos para no hacer esta inversión.

Para ello proponemos la construcción de un datacenter de respaldo, que replique todos los servicios y/o datos que el datacenter principal ofrece actualmente (virtualización). En caso de falla catastrófica, una falla parcial o un aumento circunstancial en los servicios de justicia el datacenter de respaldo puede ofrecer su capacidad para hacer frente a estos incidentes. Esta infraestructura de contingencia se conectará por medio de varios enlaces de fibra oscura.

Además de esto, el Portal WEB del Poder Judicial y la Oficina Judicial Virtual (OJV), son el principal vínculo que tiene la ciudadanía y otros actores externos (abogados) que interactúan con el PJUD, por lo que es crítico garantizar la alta disponibilidad del sitio. En consecuencia, necesariamente se debe evaluar la inversión en garantizar un sitio de contingencia que permita, en caso de catástrofe, la continuidad del servicio ofrecido. Por lo que proponemos un Hot-site, warm-site, cold-site que nos permitirán una inmensa disponibilidad del servicio frente a una contingencia. Se toma esta decisión luego de una cuidadosa consideración entre el costo y el riesgo de la medida.

Además de esto se requiere tener duplicadas las comunicaciones internas (en caso de falla), en conjunto con tener redundancia de proveedores (ISP), en el caso de corte de fibra o falla en el servicio se puede utilizar otro. Se debe verificar constantemente que los proveedores cumplan con el acuerdo de nivel de servicio (SLA) relacionado con la redundancia.

La migración es una operación crítica en la recuperación ante el riesgo, por lo que impondrán las políticas (en planes de certificar a la ISO 27002), estándares, guías, procedimientos que sean necesarios para garantizar el tiempo de respuesta mínimo para restablecer la operación (total o parcialmente) en función de las prioridades establecidas. La revisión de la políticas y las medidas, en plazos cíclicos,es vital para evaluar los resultados, obteniendo las métricas que permitan definir el grado de despliegue y adopción de las mismas en las diferentes áreas del PJUD.

Para implementar la recuperación ante desastres es necesario determinar un plan al que denominamos BCP, el cual es integral, revisa y prioriza los procesos, y decide cuáles no pueden caerse. Incluye al plan de recuperación de desastres (DRP), orientado a recuperar el centro de cómputos en caso de un desastre.

En nuestro caso de ejemplo, simplemente vamos a definir un plan de contingencias para poder ver cuál es el procedimiento para recuperarse ante el desastre.

**Plan de contingencia:** Es una estrategia que se compone de una serie de procedimientos que facilitan una solución alternativa que permite restituir rápidamente el funcionamiento de los servicios críticos de la Fundación ante la eventualidad que lo afecte de forma parcial o total.

* **Objetivo:** Establecer el Plan de Recuperación de los servicios que permita evaluar y reparar el funcionamiento del datacenter que reportó problemas eléctricos. Teniendo en cuenta que la prestación de servicios que brinda el PJUD es el activo más importante.
* **Alcance:** Este plan permitirá evaluar el estado del servicio ofrecido por el datacenter. Se indican las actividades asociadas junto con sus responsables:
* El IT manager encargado de los servicios del datacenter, reporta al Jefe de Información a través de los medios establecidos:
  + Número celular registrado en este plan.
  + Email.
  + Mensaje de texto.

Si no se recibe respuesta en menos de 4 minutos se reporta al cargo inmediatamente inferior al Jefe de Información del PJUD con los mismos medios.

El contenido de la llamada, email o mensaje contendrá la siguiente información del incidente: fecha, hora, posible causa, descripción breve de las áreas afectadas, servicios afectados, su grado de afectación, criticidad, equipamiento o personal especializado que a priori puede resolver la falla (ing. eléctrico, electromecánico etc.), período de tiempo desde el cual los servicios están afectados y tiempo aproximado para restablecer el servicio (si es estimable). El Jefe de Sistemas se comunicará por los medios establecidos:

* + - A su superior inmediato
    - A través de una notificación a las diferentes áreas afectadas

Informando sobre el incidente y dando una breve descripción de lo sucedido. Simultáneamente contactará por medios establecidos con las personas encargadas de dar respuesta posible a este percance: Jefe de Mantenimiento (en este caso), etc.

* El Jefe de Mantenimiento contactará de ser necesario al IT manager, solicitando más detalles del incidente, de tal manera de conformar el equipo idóneo para llevar a cabo el relevamiento y arreglo de los equipos afectados. Terminada la tarea de reparación, se brindará un breve informe sobre los equipos relevados, problemas detectados y causas que dieron origen al incidente, nivel de daño en los equipos, tiempo que duró la evaluación y reparación de los mismos, etc.
* EL IT manager informará por los medios establecidos al Jefe de Informática del PJUD el estado de restablecimiento de servicios, así como el tiempo total desde el momento de la falla hasta la puesta en funcionamiento del data center, y el grado y criticidad de los servicios restablecidos.
* El Jefe de Informática contactará por los medios establecidos a su superior inmediato dando un breve resumen del incidente. Y por medio de notificaciones a las diferentes áreas afectadas, las noticias sobre el incidente. Además solicitará información a cada una sobre el grado de restablecimiento del servicio y si reportan algún inconveniente con el mismo.
* El Jefe de Informática, IT manager y el Jefe de Mantenimiento se reúnen para analizar la situación y desarrollar detalladamente un plan de recuperación final o plantear posibles mejoras al plan establecido (dependiendo de la situación), esto permitirá restablecer la normalidad de los servicios en un menor tiempo.

A modo de ejemplo podemos ver en el siguiente esquema las **principales medidas de contingencias aplicadas**: Backups, redundancia de diferentes elementos críticos de IS (energía, conectividad, datos, servicios, etc.).

