UNCUYO
UNIVERSIDAD NACIONAL DE CUYO

FCE
FACULTAD DE CIENCIAS ECONÓMICAS

CONTADOR PÚBLICO NACIONAL Y PERITO PARTIDOR

SEGURIDAD INFORMÁTICA EN EL MANEJO DE LA INFORMACIÓN DE LA MUNICIPALIDAD DE LUJÁN DE CUYO

Trabajo de Investigación

POR

Noelia Belén Elías

DIRECTOR:
Prof. Pablo David Majowka

M e n d o z a-2 0 1 9

Resumen

En el presente trabajo se describe el nivel de seguridad informática que posee la Municipalidad de Luján de Cuyo de la provincia de Mendoza en el manejo de la información, para lo cual se analiza el grado de riesgo existente en la generación de los distintos tipos de daños informáticos, dado por la actuación de las amenazas sobre las vulnerabilidades y el impacto generado por las mismas. Estos aspectos se profundizan en tres ámbitos primordiales en los que pueden tener lugar: Seguridad física, seguridad lógica y seguridad en el sistema de gestión y comunicacional, señalando a su vez los tipos de delitos informáticos que existen y las conductas nocivas cometidas a través de sistemas. Se introduce cada capítulo con los conceptos y características generales de estos ámbitos y posteriormente se aborda su aplicación concreta al Municipio. Asimismo se describen las medidas de protección, políticas de seguridad y plan de contingencias adoptadas y los procedimientos, procesos y previsiones que se proponen como acciones preventivas y resultan necesarias para lograr reducir el grado de riesgo existente a niveles aceptables.

Palabras claves: Seguridad informática Municipalidad Luján de Cuyo

ÍNDICE

Introducción

Debido a que la información es un activo intangible de gran valor para cualquier organización, es que deben extremarse los esfuerzos para lograr protegerlo y garantizar de esta manera que la organización cumpla con los objetivos que se haya propuesto, resguardando a su vez, sus recursos financieros, sus sistemas, su reputación, su situación legal, y otros bienes tanto tangibles como inmateriales. Este trabajo está orientado a desarrollar las implicancias e implementaciones que surgen de la Seguridad informática y aplicarlas específicamente a la Municipalidad de Luján de Cuyo de la Provincia de Mendoza. Como objetivo general se plantea identificar el nivel de seguridad informática que posee dicha entidad, y a partir de ello la magnitud del riesgo asociado a dicho nivel con el fin de poder proponer políticas y criterios de seguridad adicionales a las existentes analizando el costo de las medidas a implantar, el valor de los bienes a proteger y la cuantificación de las pérdidas que podrían derivarse de la aparición de determinado incidente de seguridad, de esta manera se permitirá reducir dichos riesgos a un nivel aceptable.

Se plantean los siguientes objetivos específicos:

- Determinar el nivel de seguridad física (natural y humana), lógica y a nivel comunicacional (internet y sistemas) existente en el Municipio.
- Determinar el grado de riesgo de delito informático y de ciertas conductas nocivas cometidas a través de sistemas a las que el Municipio se encuentra expuesto.
- Proponer acciones preventivas adicionales a las existentes en dichos niveles que incluyan medidas de protección y políticas de seguridad adecuados para lograr reducir el grado de riesgo existente a niveles aceptables.

El presente trabajo está organizado en siete capítulos: En el primero se define la seguridad por un lado y la información por otro con el fin de poder confluir ambas definiciones y lograr una aproximación conceptual acertada de la seguridad informática, describiendo a su vez, su objetivo y conceptos fundamentales. En el segundo se analiza la seguridad física en donde primeramente se define la misma y luego se establecen los tipos de desastres de la naturaleza y las amenazas humanas, de ambos puntos se describen aspectos de seguridad específica que se relacionan con cada uno. En el tercer capítulo se habla de la seguridad lógica comenzando con la definición de las amenazas lógicas, siguiendo por los controles de acceso a tener en cuenta para mitigar dichas amenazas y finalizando con las medidas más eficientes para lograr una correcta administración de la seguridad. En el cuarto capítulo se habla de los delitos informáticos, sus elementos y características, las conductas nocivas cometidas a través de sistemas y finalmente del encuadre que ofrece la legislación nacional en este tema. En el quinto capítulo se expone la parte comunicacional

y de sistemas definiendo la estructura básica de la web y los sistemas de gestión con los aspectos de seguridad relacionados a tener en cuenta. En el sexto capítulo se disponen las acciones preventivas existentes tales como medidas de protección, políticas de seguridad y plan de contingencias. Por último en el séptimo capítulo se exponen las conclusiones de cada capítulo desarrollado anteriormente y las generales. Es importante destacar que excepto en el primer capítulo en todos los restantes, primero se ha realizado una introducción teórica de los contenidos y luego se han aplicado al caso concreto del Municipio de Luján de Cuyo.

Metodología del trabajo:

- ❖ Tipo de investigación:
  - Carácter: Cuantitativa ya que se intentará determinar el grado o nivel de seguridad informática existente mediante el análisis de diversos factores susceptibles de medición.
  - Finalidad: Aplicada ya que pretende brindar soluciones de seguridad informática perfeccionando y ampliando el plan de seguridad existente.
  - Profundidad: Descriptiva ya que busca detallar los principales aspectos a tener en cuenta sobre la seguridad informática, pero asimismo, resulta exploratoria porque se aplicará a la Municipalidad de Luján de Cuyo, la cual no posee investigaciones previas relacionadas con esta temática.
- ❖ Unidad de análisis: Seguridad informática aplicada a los sistemas informáticos existentes en la Municipalidad de Luján de Cuyo.
- ❖ Instrumentos de recolección: Se utilizará como instrumentos de recolección de datos, las siguientes fuentes primarias:
  - Observación Directa de aspectos relacionados con la seguridad física de los sistemas informáticos
  - Entrevistas abiertas y encuestas a Directivos y restante personal del Área de Informática y Comunicaciones del Municipio.
- ❖ Criterios de análisis: Se utilizará el criterio de análisis cuantitativo ya que se realizará la medición de ciertas características relacionadas con la seguridad informática para posteriormente analizar los datos obtenidos.

CAPÍTULO I:
SEGURIDAD INFORMÁTICA: CONCEPTOS BÁSICOS

Este primer capítulo incluye una introducción de conceptos fundamentales y necesarios para comprender los contenidos desarrollados en los restantes ya que se abordan los conceptos básicos de seguridad e información para luego complementar ambas definiciones y lograr una aproximación conceptual idónea y acertada del eje principal objeto del presente trabajo: La seguridad informática, la cual en capítulos posteriores se aplicará al caso concreto de la Municipalidad de Luján de Cuyo.

A. DEFINICIÓN DE SEGURIDAD

El término seguridad puede tomar diversos sentidos según el área o campo al que haga referencia. En términos generales, según Jaramillo (2017) la seguridad se define como "el estado de bienestar que percibe y disfruta el ser humano". Podría decirse que la seguridad consiste en hacer que el riesgo se reduzca a niveles aceptables, debido a que el riesgo es inherente a cualquier actividad y nunca puede ser eliminado por completo; por lo tanto el concepto de seguridad refiere a todo aquello que se protege por medio de avisos o prevenciones. La seguridad es considerada como una herramienta dentro del ámbito en que se la estudia por ser considerada por varios autores como una teoría amplia, compleja y abstracta. Como la “seguridad absoluta” no existe lo que siempre puede hacerse es aumentarla, con un proceso de mejora continua, que sirva para identificar y minimizar los riesgos constantemente y esto se logra a través de un plan de estrategias y metodologías, que sin bien no brindan la solución total (como muchos prometen), podrá cubrir parte del “agujero” que hoy se presenta al hablar de esta temática.

B. INFORMACIÓN

1. DEFINICIÓN

Se define Dato como “la unidad mínima con la que se compone cierta información”, por lo que se puede inferir que la Información es una agregación de datos que tiene un significado específico más allá de cada uno de éstos, y tendrá un sentido particular según cómo y quién la procese como resultado de la interacción con el entorno o percepciones sensibles dentro de este. En principio la información, a diferencia de los datos o las percepciones sensibles, tienen estructura útil que modificará las sucesivas interacciones del que posee dicha información con su entorno y como un elemento más del interior de

una organización, esto significa que a partir de esta se toman decisiones importantes para el desarrollo de los objetivos corporativos y, a su vez, le brindan al usuario elementos de juicio para su permanencia como cliente; de ahí, su consideración como un activo intangible muy valioso. Existe Información pública la cual puede ser visualizada por cualquier persona y aquella que debe ser privada: A la que pueden acceder un grupo selecto de personas que trabaja con ella. En esta última debemos maximizar nuestros esfuerzos para preservarla, reconociendo las características de la Información, las cuales se desarrollan a continuación.

2. CARACTERÍSTICAS

Según Borghello (2001) la información tiene las siguientes características:

La Integridad de la Información es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorias. Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificación por personas que se infiltran en el sistema.

La Disponibilidad u Operatividad de la Información es su capacidad de estar siempre disponible para ser procesada por las personas autorizadas. Esto requiere que la misma se mantenga correctamente almacenada con el hardware y el software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria.

La Privacidad o Confidencialidad de la Información: Con esta característica conseguimos que la información que estamos salvaguardando sólo pueda ser legible por parte de los usuarios autorizados, impidiendo que sea legible por terceros. En casos de falta de confidencialidad, la Información puede provocar severos daños a su dueño o volverse obsoleta.

El Control sobre la información permite asegurar que sólo los usuarios autorizados pueden decidir cuándo y cómo permitir el acceso a la misma. Asimismo si dicha información es modificada o simplemente ha sido legible por parte de los usuarios autorizados quedará registrado, logrando así que el usuario autorizado no podrá negar dicho uso, debido a dicho registro.

La Autenticidad permite definir que la información requerida es válida y utilizable en tiempo, forma y distribución. Esta propiedad también permite asegurar el origen de la información, validando el emisor de la misma, para evitar suplantación de identidades.

C. SEGURIDAD INFORMÁTICA

1. CONCEPTOS FUNDAMENTALES

Para poder comprender el concepto integral de la seguridad informática, es indispensable entender los diversos conceptos básicos que la rigen, ya que de otra forma no es posible establecer una base de estudio. Según Voutssas (2010) estos conceptos son los que se enuncian a continuación:

- Recursos Informáticos: Son el equipo de cómputo y telecomunicaciones; los sistemas, programas y aplicaciones, así como los datos e información de una organización. También se les conoce como "activos informáticos"
- Amenaza: Fuente o causa potencial de eventos o incidentes no deseados que pueden resultar en daño a los recursos informáticos de la organización.
- Impacto: La medida del efecto nocivo de un evento.
- Vulnerabilidad: Característica o circunstancia de debilidad de un recurso informático la cual es susceptible de ser explotada por una amenaza.
- Riesgo: La probabilidad de que un evento nocivo ocurra combinado con su impacto en la organización.
- Principio básico de la seguridad informática: La seguridad informática no es un producto es un proceso

2. APROXIMACIÓN CONCEPTUAL

Es necesario acoplar los conceptos y principios de seguridad expuestos anteriormente, en un contexto informático y viceversa. Para dicho cometido los expertos en seguridad y los expertos en informática deben interactuar interdisciplinariamente para lograr aproximarnos al concepto objeto del presente trabajo: Seguridad Informática, la cual se puede definir como:

> El proceso de establecer y observar un conjunto de estrategias, políticas, técnicas, reglas, guías, prácticas y procedimientos tendientes a prevenir, proteger y resguardar de daño, alteración o sustracción a los recursos informáticos de una organización y que administren el riesgo al garantizar en la mayor medida posible el correcto funcionamiento ininterrumpido de esos recursos. (Voutssas, 2010, p.5).

La seguridad de la información tiene como propósito proteger la información registrada, independientemente del lugar en que se localice: impresos en papel, en los discos duros de las computadoras o incluso en la memoria de las personas que la conocen. Es importante destacar que en la medida en que la tecnología avanza exponencialmente, las amenazas, peligros e inseguridades a los que se encuentra sujeta la información procesada y almacenada, es mucho mayor, por lo que se deberán aunar esfuerzos para lograr la formulación de estrategias adecuadas de seguridad tendientes a la disminución de dichos riesgos a un nivel aceptable, ya que como se mencionó en la definición de seguridad (Capítulo I A), la misma no puede alcanzarse en un 100% por lo tanto, es conveniente hablar del principio de "administración calculada del riesgo". Por más que la organización se esfuerce, cada

día surgen nuevas amenazas, riesgos y vulnerabilidades dentro de los activos informáticos y por lo mismo el proceso debe ser permanente y evolutivo y por lo tanto siempre será perfeccionable.

3. OBJETIVO

El objetivo de la seguridad informática apunta a lo que se pretende proteger de los diversos ataques y amenazas, éste es el denominado sistema informático, el cual se encarga de procesar la información de entrada (datos) y obtener una información de salida (resultados). Estos datos deben estar contenidos en soportes accesibles para el sistema informático y éste debe depositar los resultados del tratamiento en algún soporte comprensible para el usuario, por lo tanto en cualquier sistema informático existen tres elementos básicos a proteger: el hardware, el software y los datos.

Por hardware entendemos el conjunto de todos los sistemas físicos del sistema informático: CPU, cableado, impresoras, CD–ROM, cintas, componentes de comunicación.

Se refiere, por tanto, a los componentes materiales de un sistema informático. La función de estos componentes puede dividirse en tres categorías principales:

- Entrada
- Salida
- Almacenamiento

Los componentes de esas categorías están conectados a través de un conjunto de cables o circuitos llamado bus con la unidad central de proceso (CPU) del ordenador.

El software son todos los elementos lógicos que hacen funcional al hardware: sistema operativo, aplicaciones, utilidades, etc.

En un sentido más amplio Software engloba a todo lo que convierte al ordenador en una máquina capaz de obtener resultados.

Existen dos tipos de software: Sistemas operativos y Software de gestión.

El sistema operativo es un conjunto de programas que constituyen la "inteligencia básica" del ordenador. Tiene dos objetivos fundamentales: El primero es "dar vida" a la máquina, es decir, convertir el conjunto de dispositivos interconectados en un ordenador capaz de dialogar con el mundo exterior, con el usuario. El segundo de los objetivos es gestionar de la forma más eficaz los recursos físicos del ordenador.

El software de gestión es el conjunto de programas que permiten transformar el ordenador en una herramienta capaz de resolver tareas específicas.

Por último entendemos por datos al conjunto de información lógica que maneja el software y el hardware: bases de datos, documentos, archivos.

Para concluir se puede decir que el objetivo primario de la seguridad informática es mantener al mínimo los riesgos sobre los recursos informáticos, –todos los recursos– y garantizar así la continuidad de las operaciones de la organización al tiempo que se administra ese riesgo informático a un cierto costo aceptable. El objetivo secundario consiste en garantizar que los documentos, registros y archivos informáticos de la organización mantengan siempre su confiabilidad total.

Recapitulando lo expuesto en este capítulo es importante destacar que para lograr una aproximación conceptual idónea de seguridad informática es necesario congeniar los conceptos y principios de seguridad, en un contexto informático y viceversa sin dejar de lado para dicha aproximación un aspecto fundamental a tener en cuenta: el sistema informático que resulta ser lo que se pretende proteger.

CAPÍTULO II:
SEGURIDAD FÍSICA

En el presente capítulo se analizarán los tipos de desastres de la naturaleza y amenazas humanas que contribuyen a vulnerar la seguridad física de los sistemas informáticos, para luego poder describir las medidas que se deben implementar para lograr que el nivel de este tipo de seguridad aumente. Al final del capítulo todos los puntos expuestos se aplican el caso específico de la Municipalidad de Luján de Cuyo.

A. DEFINICIÓN

La Seguridad Física consiste en la "*aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial*" (Huerta, 2000). Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos. Evaluar y controlar permanentemente la seguridad física del sistema es la base para comenzar a integrar la seguridad como función primordial del mismo. Tener controlado el ambiente y acceso físico permite disminuir siniestros y tener los medios para luchar contra accidentes.

B. TIPOS DE DESASTRES O AMENAZAS Y SEGURIDAD ASOCIADA A LOS MISMOS

Las principales amenazas que se prevén en la seguridad física son:

1. Terremotos, inundaciones, incendios accidentales, tormentas, picos de tensión, etc. (Seguridad Ambiental)
2. Amenazas ocasionadas por el hombre. (Seguridad en los accesos)

1. DESASTRES DE LA NATURALEZA Y SEGURIDAD AMBIENTAL

La seguridad ambiental hace referencia a los procedimientos, procesos y previsiones que se deben de tener en cuenta a fin de controlar los efectos de la naturaleza, los cuales pueden dañar seriamente a los equipos informáticos, al personal de la entidad y lo más importante, a los datos de la empresa. A continuación se nombran los principales accidentes que pueden ocurrir en este ámbito:

a.Terremotos

Debido a que cada sistema es único, la política de seguridad a implementar no será uniforme para todos ellos. Este concepto vale, también, para el edificio en el que nos encontramos. Es por ello que siempre se recomendarán pautas de aplicación general y no procedimientos específicos. En el caso de los terremotos, depende mucho de la situación geográfica de la entidad, por ejemplo, si estuviéramos en un país como Japón donde los mismos están a la orden del día sería totalmente necesaria y fundamental dicha inversión, pero si fuese como en el caso de España, donde nunca se da ningún terremoto importante ya que sus posibilidades son mínimas, dichas inversiones serán menores.

En este caso se recomienda no situar nuestros equipos o sistemas informáticos cerca de las ventanas o en superficies altas por miedo de sus posibles caídas, se recomienda el uso de fijaciones. Por supuesto tampoco hay que colocar objetos pesados encima de los equipos por miedo a provocar daños en dichos equipos.

También se recomienda el uso de plataformas de goma las cuales absorben parte de las vibraciones generadas por los terremotos, además del uso de mesas anti vibraciones ya que sin ellas se podrían dañar los discos duros donde se guarda información vital.

b.Inundaciones

Se las define como la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial. Esta es una de las causas de mayores desastres en centros de cómputos. Además de las causas naturales de inundaciones, puede existir la posibilidad de una inundación provocada por la necesidad de apagar un incendio en un piso superior.

Para evitar este inconveniente se puede construir un techo impermeable para evitar el paso de agua desde un nivel superior y acondicionar las puertas para contener el agua que bajase por las escaleras.

Estos problemas son graves ya que son los que más daño hacen a la entidad, debido a que cualquier sistema eléctrico en contacto con el agua queda automáticamente inutilizado, bien por el propio líquido o bien por los cortocircuitos que genera en los sistemas electrónicos, además puede ser mortal para los empleados de la entidad.

Se recomienda el uso de detectores de agua los cuales al dispararse la alarma corten automáticamente la corriente eléctrica para evitar males mayores. Es importante destacar que los equipos deben estar por encima del sistema de detección de agua, sino cuando se intente parar ya estará mojado. Para su detención se recomienda avisar a las autoridades competentes (bomberos, policía, etc.)

con el fin de socorrernos de la manera más adecuada y en forma profesional, ya que tendrán que cortar la corriente eléctrica, en caso de que nuestro sistema de seguridad no haya podido hacerlo por lo que nunca deberá hacerlo personal de la entidad.

c.Fuegos (incendios)

Los incendios son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas.

El fuego es una de las principales amenazas contra la seguridad. Es considerado el mayor enemigo de las computadoras ya que puede destruir fácilmente los archivos de información y programas.

Se recomienda el uso de alarmas, las cuales al detectar fuego o humo, se activan directamente los extintores que están situados en el techo y avisan a las autoridades con el fin de evitar males mayores.

También es necesario el uso de extintores de mano que estén repartidos por toda la entidad; al lado de los mismos deben existir carteles anunciado su presencia e indicando su situación.

d.Tormentas eléctricas

Las tormentas eléctricas pueden ocasionar graves daños físicos a la entidad. Estos daños pueden ser desde fuegos ocasionados por las tormentas hasta picos de tensión los cuales pueden destrozar nuestros equipos informáticos con sus respectivos datos.

Se recomienda el uso de pararrayos, éstos consisten en una varilla de metal, puesta en el tejado o en la parte más elevada del edificio de la entidad, la cual tiene un cable de cobre que va a parar a una plancha del mismo metal introducida a unos metros bajo tierra. En caso de que un rayo toque el pararrayos este de descargará al tocar tierra, evitando posibles daños.

Además se recomienda que las copias de seguridad que se realicen estén siempre alejadas de las estructuras metálicas del edificio de la entidad.

e.Picos de tensión

Trabajar con computadoras implica trabajar con electricidad. Por lo tanto esta una de las principales áreas a considerar en la seguridad física. En la medida que los sistemas se vuelven más complicados se hace más necesaria la presencia de un especialista para evaluar riesgos particulares y aplicar soluciones que estén de acuerdo con una norma de seguridad industrial.

Los picos de tensión son otros problemas que puede tener cualquier entidad, los cuales pueden provocar pequeños daños a nuestros equipos informáticos.

Se recomienda el uso de SAIs, (sistema de alimentación ininterrumpida), con los cuales en caso de que exista un pico de tensión mantendrá al equipo en un estado a salvo de cualquier posible daño.

2. AMENAZAS HUMANAS

Las personas son la principal fuente de amenaza que existe en los sistemas de información y son el tipo de amenaza en el que se invierten más recursos para controlarlos y contrarrestar sus efectos.

Dichas amenazas abarcan actos malintencionados, incumplimiento de las medidas de seguridad como consecuencia de actos negligentes o falta de controles adecuados pudiéndose resumir en las siguientes:

- Robo

Las computadoras son activos valiosos de las empresas y están expuestas, de la misma forma que lo están las piezas de stock e incluso el dinero. Es frecuente que los trabajadores utilicen la computadora de la empresa para realizar trabajos privados o para otras organizaciones y, de esta manera, robar tiempo de máquina. La información importante o confidencial puede ser fácilmente copiada o robada directamente de los discos que los contienen.

El software, es una propiedad muy fácilmente sustraíble y las cintas y discos son fácilmente copiados sin dejar ningún rastro.

- Fraude

El fraude o estafa informática es el uso de una computadora con el objetivo de distorsionar datos para inducir a otra persona a que haga o deje de hacer algo que ocasiona una pérdida. Los delincuentes pueden distorsionar los datos de diferentes maneras: Primero, pueden alterar sin autorización los datos ingresados en la computadora (los empleados pueden usar fácilmente este método para alterar esta información y malversar fondos). En segundo lugar, los delincuentes pueden alterar o borrar información almacenada. Tercero, los delincuentes sofisticados pueden reescribir los códigos de software y cargarlos en la computadora central de un banco para que éste les suministre las identidades de los usuarios utilizando esta información para realizar compras no autorizadas con tarjetas de crédito por ejemplo.

Cada año, millones de dólares son sustraídos de empresas y, en muchas ocasiones, las computadoras han sido utilizadas como instrumento para dichos fines.

Sin embargo, debido a que ninguna de las partes implicadas (compañía, empleados, fabricantes, auditores, etc.), tienen algo que ganar, sino que más bien pierden en imagen, no se da ninguna publicidad a este tipo de situaciones.

- Sabotaje

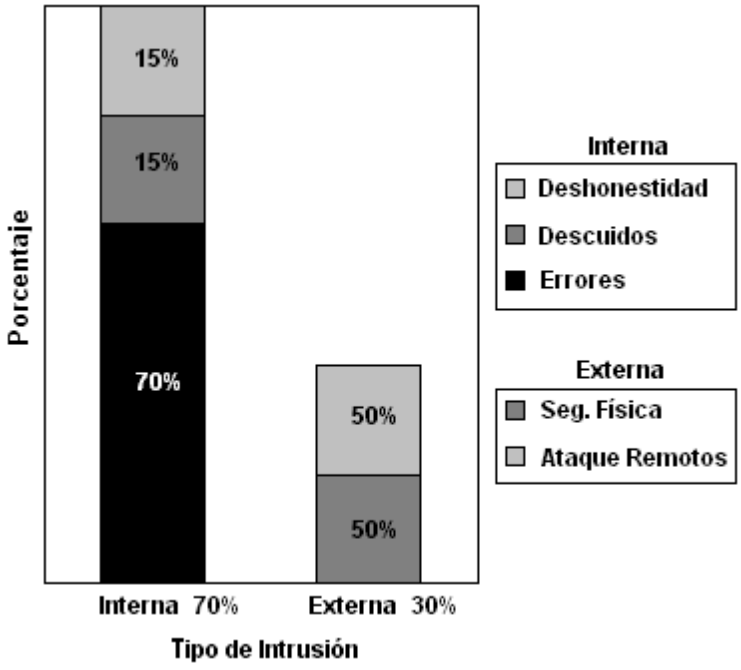
El sabotaje informático desde el punto de vista de la “destrucción física de los elementos del equipo” comprende a todo tipo de conductas destinadas justamente a la destrucción "física" del hardware y el software de un sistema (por ejemplo: causar incendios o explosiones, introducir piezas de aluminio dentro de la computadora para producir cortocircuitos, echar alguna bebida o agentes cáusticos en los equipos, etc.).

En este punto podemos decir que los casos en que se han detectado sabotajes causados mediante el incendio o la colocación de bombas, son realizados generalmente por personas extrañas a la entidad donde funciona el sistema pero también pueden ser ocasionados por un empleado de la misma. Es el peligro más temido en los centros de procesamiento de datos.

Físicamente, los imanes son las herramientas a las que se recurre, ya que con una ligera pasada la información desaparece, aunque las cintas estén almacenadas en el interior de su funda de protección. Una habitación llena de cintas puede ser destruida en pocos minutos y los centros de procesamiento de datos pueden ser destruidos sin entrar en ellos. Además, suciedad, partículas de metal o gasolina pueden ser introducidos por los conductos de aire acondicionado, las líneas de comunicaciones y eléctricas pueden ser cortadas, etc.

Las amenazas se pueden dividir en externas e internas, en el gráfico siguiente se muestran las causas principales por las que se cometen unas u otras:

Imagen 1: Tipos de intrusiones



Fuente: http://www.cybsec.com

a. Amenazas Externas

Son aquellas amenazas humanas cuyo autor es más común que se encuentre afuera de la organización. Al no tener información certera de la red interna de la empresa, el atacante tiene que realizar ciertos pasos para poder conocer qué es lo que hay en ella y buscar la manera de atacarla. La buena noticia en este tipo de amenazas informáticas es que pueden ser evitadas desde el interior de la empresa si se tienen las medidas de seguridad correctas.

b. Amenazas Internas (Personal)

Son las amenazas a la seguridad de un sistema, provenientes del personal del propio sistema informático, las que rara vez son tomadas en cuenta porque se supone un ámbito de confianza muchas veces inexistente. Generalmente estos ataques son accidentes por desconocimiento o inexistencia de las normas básicas de seguridad; pero también pueden ser del tipo intencional ya que la mayor amenaza de fraude proviene de sus áreas internas, perpetrado por algún miembro de la propia organización. Tengamos en cuenta que la pérdida de confidencialidad y privacidad de la información además de tener como consecuencia aspectos económicos adversos para la organización, también le crea expuestos legales y de imagen ante la comunidad, por lo que la creación de una base para el desarrollo de métodos y procedimientos para determinar la efectividad de los controles requiere que se discutan conceptos de gestión de riesgos asociados a los recursos humanos de toda la organización.

Algunos grupos de personas que se pueden mencionar en esta sección son las siguientes:

- Exs–Empleados: Este grupo puede estar especialmente interesado en violar la seguridad de la empresa, sobre todo aquellos que han sido despedidos y han quedado disconformes; o bien aquellos que han renunciado para pasar a trabajar en la competencia. Generalmente se trata de personas descontentas con la organización que conocen a la perfección la estructura del sistema y tienen los conocimientos necesarios como para causar cualquier tipo de daño.

- Curiosos: Suelen ser los atacantes más habituales del sistema. Son personas que tienen un alto interés en las nuevas tecnologías, pero aún no tienen los conocimientos ni experiencia básicos para considerarlos hackers o crackers. En la mayoría de los casos son estudiantes intentando penetrar los servidores de su facultad o empleados consiguiendo privilegios para obtener información para él vedada. Generalmente no se trata de ataques de daño pero afectan el entorno de fiabilidad con confiabilidad generado en un sistema.

- Intrusos Remunerados: Este es, sin duda, el grupo de atacantes más peligroso, aunque también el menos habitual. Se trata de crackers o piratas con grandes conocimientos y experiencia, pagados por

una tercera parte para robar “secretos” (código fuente de programas, bases de datos de clientes, información confidencial de satélites, diseño de un nuevo producto, etc.) o simplemente para dañar, de alguna manera la imagen de la entidad atacada. Suele darse, sólo, en grandes multinacionales donde la competencia puede darse el lujo de un gran gasto para realizar este tipo de contratos y contar con los medios necesarios para realizar el ataque.

A continuación se desarrollan los tipos de controles a tener en cuenta para lograr mitigar el riesgo ocasionado por las amenazas humanas:

3. CONTROL DE ACCESOS

El control de accesos es una forma de lograr que solo las personas autorizadas puedan acceder a un determinado equipamiento informático, para esto las organizaciones utilizan una gran variedad de herramientas y técnicas con el fin de identificar a su personal autorizado. Los controles de acceso puede ser autónomos o en red, los primeros son mecanismos que permiten restringir o administrar de manera segura el acceso físico a un espacio o instalación. Este tipo de control opera mediante la introducción de una clave de acceso, una tarjeta magnética o incluso a través del uso de patrones biométricos, como la lectura ocular, el reconocimiento facial o el marcaje de la huella dactilar. En el caso del control de acceso en red, este funciona de manera integrada por medio de una PC o equipo informático de similares características, el cual puede ser operado de manera local o también remota, por lo tanto debe contarse con un software de control, especialmente desarrollado para llevar un registro efectivo y fidedigno de todas las incidencias que pueden suscitarse, incluyendo fecha y horario de las mismas, además de la identificación de cada usuario. A continuación se detallan algunos de los controles autónomos y de red que pueden existir:

- **Controles autónomos**
  - **Guardias**

El Servicio de Vigilancia es el encargado del control de acceso de todas las personas al edificio. Este servicio es el encargado de colocar los guardias en lugares estratégicos para cumplir con sus objetivos y controlar el acceso del personal. A cualquier personal ajeno a la planta se le solicitará completar un formulario de datos personales, los motivos de la visita, hora de ingreso y de egreso, etc. El uso de credenciales de identificación es uno de los puntos más importantes del sistema de seguridad, a fin de poder efectuar un control eficaz del ingreso y egreso del personal a los distintos sectores de la empresa. En este caso la persona se identifica por algo que posee como por ejemplo: una llave, una tarjeta de identificación con una foto o una tarjeta inteligente que contenga una identificación digital codificada almacenada en un chip de memoria. Cada una de ellas tiene un PIN (Personal Identification

Number) único, siendo este el que se almacena en una base de datos para su posterior seguimiento, si fuera necesario. Su mayor desventaja es que estos elementos pueden ser copiados, robados, etc., permitiendo ingresar a cualquier persona que la posea. Las personas también pueden acceder mediante algo que saben (por ejemplo una contraseña, un número de identificación o una combinación de bloqueo) que se solicitará a su ingreso. Al igual que el caso de las tarjetas de identificación, los datos ingresados se contrastarán contra una base donde se almacena los datos de las personas autorizadas. Este sistema tiene la desventaja que generalmente se eligen identificaciones sencillas, bien se olvidan dichas identificaciones o incluso las bases de datos pueden verse alteradas o robadas por personas no autorizadas.

- **Sistemas biométricos**

Definimos a la Biometría como el estudio para el reconocimiento inequívoco de personas basado en uno o más rasgos conductuales o físicos intrínsecos, que no son mecánicos. La biometría informática es la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo, para su autentificación, es decir, verificación de su identidad. La forma de identificación consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una base de datos. Algunas características físicas son las manos, los ojos, las huellas digitales, la voz, entre otras. Pueden eliminar la necesidad de poseer una tarjeta para acceder como también los inconvenientes de tener que recordar una password o un número de PIN de acceso, garantizando de esta forma, uno de los niveles de autenticación menos franqueables en la actualidad. A su vez tienen la ventaja que al estar relacionados de forma directa con el usuario, son exactos y permiten hacer un rastreo de auditorías. Asimismo utilizando un dispositivo biométrico los costos de administración son más pequeños, ya que se realiza el mantenimiento del lector, y una persona se encarga de mantener la base de datos actualizada.

- **Controles en red**

  - **Protección Electrónica**

La seguridad electrónica es la aplicación de las Tecnologías de la Información y la Comunicación (TIC) a las actuaciones de seguridad física. De esta manera se detectan robos, intrusiones, asaltos e incendios mediante la utilización de sensores conectados a centrales de alarmas, por lo tanto permiten la protección activa, la protección pasiva, la señalización y el alumbrado de emergencia o la megafonía de emergencia y evacuación. Estas centrales tienen conectadas los elementos de señalización que son los encargados de hacerles saber al personal de una situación de emergencia. Cuando uno de los elementos sensores detectan una situación de riesgo, éstos transmiten inmediatamente el aviso a la central; ésta procesa la información recibida y ordena en respuesta la emisión de señales sonoras o

luminosas alertando de la situación. Algunos de los sistemas de seguridad electrónica son: Circuitos cerrados de televisión en donde los monitores de estos circuitos deben estar ubicados en un sector de alta seguridad ya que la importancia de la video vigilancia es evidente por ser una herramienta de ayuda a la reducción del número de delitos. La mayoría de las cámaras utilizadas son de alta definición y se conectan con las redes existentes vía protocolos IP. Incluyen muchas opciones para comparar objetos de forma automática por sus características y para programarlas a fin de que desencadenen acciones en función de dichas imágenes. Otro sistema es el de los detectores pasivos sin alimentación los cuales sólo van conectados a la central de control de alarmas para mandar la información de control, algunos ejemplos son: detector de aberturas (contactos magnéticos externos o de embutir), Detector de roturas de vidrios (inmune a falsas alarmas provocadas por sonidos de baja frecuencia; sensibilidad regulable) y Detector de vibraciones (detecta golpes o manipulaciones extrañas sobre la superficie controlada). Por último podemos mencionar el sistema de sonorización y dispositivos luminosos dentro de los cuales podemos encontrar sirenas, campanas, timbres, faros rotativos, balizas, luces intermitentes, etc. Estos deben estar colocados de modo que sean efectivamente oídos o vistos por aquellos a quienes están dirigidos. Los elementos de sonorización deben estar bien identificados para poder determinar rápidamente de qué tipo de alarma se trata.

C. SEGURIDAD FÍSICA EN LA MUNICIPALIDAD DE LUJÁN DE CUYO

1. SEGURIDAD AMBIENTAL

En cuanto a la seguridad ambiental la organización posee cortafuegos especiales los cuales poseen el mantenimiento periódico efectuado por la Dirección de Medicina, Higiene y Seguridad laboral del Municipio de acuerdo a norma IRAM 3517. Este mantenimiento consiste en una recarga anual y en una prueba hidráulica como se puede visualizar en la imagen 2.

Imagen 2: Extintor área informática

La organización no posee detectores de humo ni protección contra tormentas eléctricas. Para la seguridad del personal, la Municipalidad posee 2 tomas de tierra, uno se encuentra destinado al grupo electrógeno ubicado en el patio del Edificio Municipal de calle Taboada (Imagen 3) y el otro a la oficina general de informática.

Imagen 3: Grupo electrógeno patio edificio Taboada

Este grupo electrógeno, ante un corte de energía, alimenta al servidor de la oficina central

(Imagen 4), el rack central y el otro servidor localizado en la oficina de Defunciones el cual une los dos edificios.

Imagen 4: Servidor oficina central

Para lograr una energía ininterrumpida también se poseen 2 UPS destinados a los servidores y uno por cada PC ubicada en la oficina central. Estos otorgan un lapso de 15 minutos para guardar los archivos abiertos ante un corte de energía.

Para la climatización de los servidores se posee un aire acondicionado de 6000 frigorías que funciona permanentemente y otro de igual cantidad de frigorías de repuesto. La oficina central posee otro de menor magnitud.

De acuerdo a las conversaciones mantenidas los ductos tienen una infraestructura adecuada.

2. SEGURIDAD DE ACCESOS

Para el edificio ubicado en calle Taboada existen ciertas medidas de seguridad para la oficina general de informática donde se encuentran los servidores. Estas medidas son: cerrojo eléctrico en la puerta de ingreso, mantener cerrado con llave cuando se retira el personal y 2 cámaras de vigilancia ubicadas una en dicho ingreso y la otra en el patio.

Por otra parte a través de la solicitud n° 675/2019 el Municipio inició la contratación de un sistema de control de accesos de personal y vehicular destinado al Edificio ubicado en calle Boedo 385

de Carrodilla (Parque Cívico), edificio al cual se trasladarán el 90% de las oficinas municipales que actualmente se encuentran repartidas en el centro de Luján de Cuyo.

Dicho Sistema se compone de puntos de accesos del personal, puertas inteligentes, acceso vehicular, sistema hardware para monitoreo de cámaras y registro de tránsito de acceso, sistema de software operativo de funcionamiento permanente compatible con el sistema biométrico de control de asistencia vigente al igual que el de Gestión Informática Municipal.

El pliego de dicha contratación tuvo las siguientes condiciones:

"Cada oferente deberá presentar su oferta de prestación de servicios teniendo en cuenta que el software y hardware necesarios o propuestos ofrezcan la mejor integración con los sistemas de gestión de personal que utiliza el municipio y los sistemas de seguridad que opera el centro de monitoreo municipal.

Atento lo expuesto, se planea tres secciones fundamentales dentro de este sistema de control de acceso: Sección de accesos peatonales, Sección de accesos vehiculares y Sección de sistemas integrales de gestión.

- Accesos Peatonales:

Se montará 1 (un) Acceso Peatonal: El mismo estará compuesto por 3 (tres) molinetes/torniquetes con lectores integrados para tarjetas RFID, además de l (una) puerta para discapacitados con lector integrado. Debe contemplarse el acceso bidireccional por puerta y molinete de invitados y visitantes con lector RFID y buzón de retorno para tarjetas, las cuales permanecerán cerradas para evitar accesos no autorizados.

Los molinetes deben contar con un sistema de seguridad (que se desbloqueen, abatan o caigan) ante corte de energía o emergencias, de modo que aseguren que los usuarios salgan sin inconvenientes y que se comuniquen con el sistema de alarma de incendios para la funcionalidad, deberán también poseer una batería para su autonomía.

Puertas con cerraduras Inteligentes: Se instalará un sistema de cerraduras inteligentes en distintas puertas de acceso. Las mismas podrán contar con formas de desbloqueo más convenientes en función de la integración general (Huella Digital/Tarjeta RFID, etc.). Deberá contar con registro de ingreso y egreso y adaptarse a todas las direcciones de apertura, asimismo deberá contar con desbloqueo en caso de emergencia. Los datos de almacenamiento deberán permanecer inalterables y deberán posibilitar el funcionamiento normal inclusive ante pérdida de corriente, desconexión de la red de datos, emergencias, etc. Debe incluir alarma inteligente para detectar operaciones no autorizadas, puerta abierta, problemas técnicos etc. Las cerraduras deben ser del tipo electromagnéticas de por lo menos 250 kg y deben contar con monitor de puerta abierta. Debe contar con alimentación ininterrumpida con baterías de respaldo para asegurar el funcionamiento ante cortes de energía eléctrica.

En cada uno de los puestos de accesos peatonales y puertas inteligentes se deberán instalar cámaras de alta definición las cuales se conectarán a videograbadoras o servicios de grabación de video para luego ser gestionadas y visualizadas en centro de monitoreo. El acceso al edificio de intendencia deberá contar

con un sistema de video portero integrado al sistema de grabación y gestión de video que permita la operación de la recepcionista y además la gestión integral desde el centro de monitoreo pudiendo establecer video comunicaciones tanto con la puerta como con la recepcionista.

- Acceso Vehicular

Se montaran 3 (tres) Puestos de Accesos Vehiculares: los mismos estarán compuestos por 06 (seis) barreras vehiculares automatizadas para ingreso/egreso, de diseño resistente de larga vida, con apertura y cierre manual/automatizada en lo posible deberá contar con semáforo incorporado que indica si el vehículo está habilitado o no para traspasarla, controlador electrónico con microprocesador, interruptor de accionamiento manual, liberación de mecanismo en caso de corte de energía, montaje izquierdo o derecho. Además se incorporarán en forma conjunta un Lector RFID para el ingreso de vehículos registrados con tarjetas.

Se instalará 1 (un) ingreso/egreso de Parking compuesto de: módulo Expendedor de Acceso mediante impresión de ticket/Acceso mediante tarjeta de proximidad RFID/Acceso mediante lectura de código/A través del móvil mediante Bluetooth con cámara led para lectura de patente incluida, etc., para el Ingreso Vehicular y otro módulo de lectura de ticket para el Egreso Vehicular de iguales características pero con función de comprobación de Tickets y las otras formas de Acceso antes mencionadas. Cabe aclarar que estos equipamientos se instalarán en forma conjunta con las barreras vehiculares. Se deberá contemplar el control mediante tarjeta RFID de un portón automatizado adicional que deberá integrarse al sistema de control de acceso vehicular. En cada uno de los Puestos de Accesos Vehiculares se deberá instalar cámaras de alta definición las cuales se conectarán a video grabadoras o servicios de grabación de video para luego ser gestionadas y visualizadas en centro de monitoreo.

- Sistema integral de gestión.

Para aunar las tecnologías de biometrías, móviles, dispositivos, etc. es necesario poseer software y hardware compatibles y con unificación de criterios de comunicación.
Se adquirirá un Software de gestión de dispositivos y de usuarios donde se gestionen niveles de accesos, tarjetas de visita, grupos de puestos y usuarios del sistema integrando diversos sistemas como el de Asistencia, Control de accesos, Cámaras, Seguridad, sistema de incendio, etc. por medio de interfaces se logrará personalizar y ajustar el Sistema de Control a nuestras necesidades con una misma plataforma.

Características básicas: Software de Seguridad y Control de Accesos: Un Software de Control de Acceso Integral con características específicas debe permitir ser programado para diferentes tipos de accesos y usuarios. Debe contar con visualización y registro de eventos y transacciones en tiempo real debiendo permitir la localización de usuarios por zonas/áreas. Además contar con campos libres para personalizar las fichas de usuarios. Permitir un aumento de la seguridad con el uso de identificación biométrica de huellas digitales. Deberá poseer multiprotocolo de lectores Radio, Wiegand, Magnético, Código de Barras, biométrico, etc. Soportar múltiples estaciones de trabajo. Poseer Bases de datos en

MS® Access o SQL sobre servidor con MS® SQL Server. Deberá permitir la definición de múltiples grupos de acceso. Permitir el control de visitantes. Permitir el despliegue de fotografía de los usuarios. Permitir el monitoreo gráfico de alarmas en tiempo real. Poseer sistema de Gestión de cámaras y grabadores. Además contar con Niveles de Seguridad. Admitir Copia de Segundad. Mostrar Niveles de Crisis. Escolta. Trampa (Interbloqueo). Poseer control de Anti- Passback Local, Temporizado y Global. Contar con Módulo Gráfico para gestión gráfica de Alarmas. Contar con Módulo de Control de Presencia. Contar con Módulo de Administración de Estacionamientos de Vehículos. Contar con Módulos opcionales de Control de Ascensores, control de Ronda de Guardia, de CCTV Deberá contar infraestructura o múltiples sitios remotos vía MODEM, RS232, RS485 o TCP.

Sera importante la integración y compatibilidad que se logre con los sistemas de control de personal con los que se cuenta y con el sistema de gestión municipal.

El sistema de parking deberá contar con la posibilidad de funcionamiento autónomo con plazos de vencimiento de ticket configurables y la incorporación de un sistema de control de estacionamiento con plataforma web, multiusuario, multi-caja soportado por base de datos Mysql, ampliamente parametrizable en fundón de futuras necesidades de gestión del estacionamiento.

Adquisición de Grabadoras de tipo DVR/NVR/HVR con SO embebido/Vms "Video Management Software" capaz de gestionar múltiples cámaras, enconders, grabadoras, alarmas, etc.

Sistema de Parking: Emisor de comprobante para sistemas de estacionamiento. Totalmente construido en gabinete de hierro con pintura epoxi fosfatizado, apto para ser utilizado en intemperie. Ampliamente configurable. Impreso térmico de alto rendimiento con presentador de ticket y censado de presencia de papel en boquilla. Tapa posterior para recambio de papel y montaje. Modo de funcionamiento autónomo. Comunicación Ethernet. Anulación automática de los tickets no retirados. Lector de tarjeta de proximidad para abonados. Lámpara para ubicación nocturna. Salida de comandos para barrera vehicular y semáforo. Entrada para sensores de barrera baja, altura de vehículo, pulsador, falta de papel, detector vehicular. Carga adicional para rollo de 150 mm de diámetro.

Lector de salida de estacionamiento en gabinete de hierro con pintura epoxi fosfatizado, apto para ser utilizado en intemperie. Funcionamiento autónomo. Comunicación Ethernet. Lector láser Incorporado con un haz / multi haz omnidireccional. Anulación automática de los tickets no retirados. Lector de tarjeta de proximidad para abonados. Lámpara para ubicación nocturna. Salida de comandos para barrera vehicular y semáforo. Entrada para sensores de barrera baja y detector vehicular.

Sistema de control de accesos: Control accesos en red para accesos completos (entrada y salida). Comunicaciones a través de Ethernet TCP/IP o RS-485. Capacidad de hasta 3.000 huellas, 30.000 tarjetas RFID y 100.000 eventos en forma local. Procesador de 32 bits a 400 MHZ, con 32MB de memoria RAM y 128MB de memoria flas Salidas de relé de puerta y auxiliares, se pueden utilizar para un control adicional a una interfaz de luces, alarmas, paneles de detección de intrusos, dispositivos de cierre extra o incluso otros controladores. Puertos de lectura weigand y RS485. Puertos de entrada

Botones de salida, sensores de puerta y entradas auxiliares. Puertos de salida: relé para cerradura y relé para salida auxiliar.

Software de gestión: Plataforma de segunda basada en web 'Todo en Uno". Múltiples módulos integrados de Acceso Tiempo, Elevadores (Conectado/ Desconecte), control de visitantes de estacionamiento para patrullaje y video con una arquitectura de sistema de identificación biométrica de alto nivel y una interfaz de usuario moderna.

Sistema Portero Visor: Compuesto por un frente con cámara y un monitor Cámara de 1 Mp con vidrio templado resistente al agua 365 Visión nocturna: la luz blanca en la cámara permite mite mostrar una imagen clara durante la noche. Botón con luz posterior, fácil de operar.

Llamadas a monitor interno y centro de administración. Apertura con tarjeta IC. Soporta apertura remota Soporta llamadas personalizadas. Soporta module extensión de control de acceso. Parta TFT táctil capacitiva de 7 pulgadas. Soporta 8 entradas de alarmas cableadas. Soporta Hamacas entre monitores. Soporta fotos y llamada durante la vigilancia. Soporta estacione; exteriores y monitor IPC. Soporta mensajes de audio y video. Soporta alimentación PoE Soporta Micro SD para grabación de video y fotos.

Sistema de video seguridad: Sistema penta híbrido (CVBS/FIDCVI/AHD/TVI/IP self-adaptive), Comunicaciones a través de Ethernet TCP P. Cámaras Megapixel, lente 2.8mm, distancia 30m, DC12V, IP67, metálicas.

Adquisición: El proyecto total, incluye 15 (quince) controles de acceso distribuidos en 11 (once) PUNTOS de CONTROL (Accesos Peatonales, Puertas Inteligentes, Barreras Vehiculares y portón automatizado), dentro del Edificio ubicado en Calle Boedo 385 de Carrodilla y en la Playa de Estacionamiento del mismo. El oferente deberá incluir en la propuesta los esquemas de instalación para que sean incluidos en el proyecto de obra civil.

En definitiva, de acuerdo a lo detallado en el capítulo se deben tener en cuenta los potenciales desastres de la naturaleza de la zona geográfica en donde se encuentren los sistemas informáticos a proteger para poder implementar las medidas adecuadas, así como también la preponderante amenaza que implica el factor humano en la seguridad física debiéndose hacer especial énfasis en la calidad de los controles de accesos a implementar.

CAPÍTULO III:
AMENAZAS Y SEGURIDAD LÓGICA

En el presente capítulo se abordan las amenazas lógicas que sufren los sistemas informáticos, las cuales se pueden manifestar a través de distintos tipos de ataques. Ante dichas amenazas se definen los controles de acceso internos y externos que deberán implementarse como medidas de seguridad y en qué consiste una eficiente administración de seguridad lógica. El capítulo culmina con el análisis de estos aspectos aplicados a la institución en cuestión.

A. AMENAZAS LÓGICAS

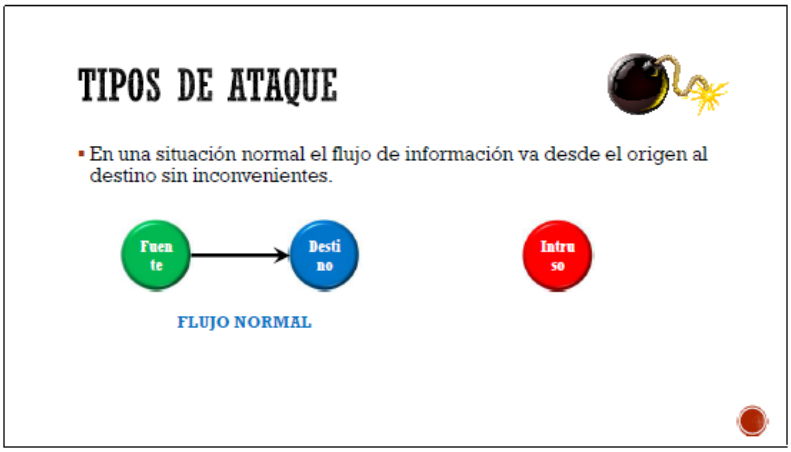
Bajo la etiqueta de "amenazas lógicas" encontramos todo tipo de programas que de una forma u otra pueden dañar a nuestro sistema, creados de forma intencionada para ello (software malicioso, también conocido como malware) o simplemente por error (amenaza más habitual). Esta última puede generar que una situación no contemplada a la hora de diseñar un sistema de red o un error accediendo a memoria en un fichero comprometa local o remotamente a cualquier sistema operativo.

A estos errores de programación se les denomina bugs, y a los programas utilizados para aprovechar uno de estos fallos y atacar al sistema, exploits, los que son utilizados para acceder a archivos, obtener privilegios o realizar sabotaje. Estas vulnerabilidades ocurren por variadas razones, y miles de "puertas invisibles" son descubiertas cada día en sistemas operativos, aplicaciones de software, protocolos de red, browsers de Internet, correo electrónico y toda clase de servicios informáticos disponibles.

La identificación de amenazas requiere conocer entre otras cosas los tipos de ataques, los cuales se clasifican en los siguientes:

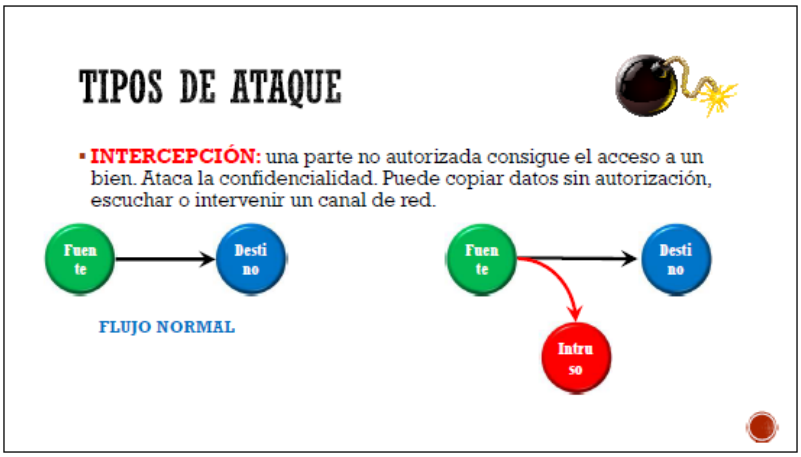
1. TIPOS DE ATAQUE

Imagen 5: Tipos de ataque: Situación Normal



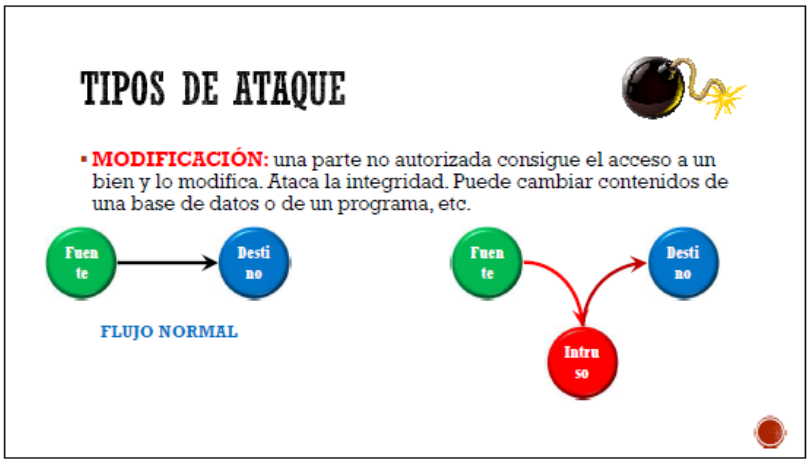
Fuente: Cátedra Auditoría Operativa y de Sistemas Computarizados-FCE-UnCuyo

Imagen 6: Tipos de ataque: Intercepción



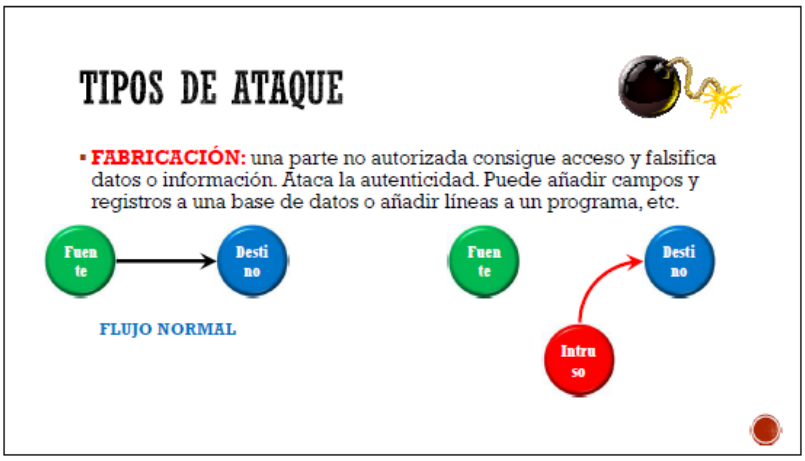
Fuente: Cátedra Auditoría Operativa y de Sistemas Computarizados-FCE-UnCuyo

Imagen 7: Tipos de ataque: Modificación



Fuente: Cátedra Auditoría Operativa y de Sistemas Computarizados-FCE-UnCuyo

Imagen 8: Tipos de ataque: Fabricación



Fuente: Cátedra Auditoría Operativa y de Sistemas Computarizados-FCE-UnCuyo

B. CONCEPTO Y OBJETIVOS DE LA SEGURIDAD LÓGICA

Otro tipo de seguridad a considerar, cuando hablamos de seguridad informática, es la Seguridad lógica. Piattini Velthuis y Del Peso Navarro en su libro "Auditoría práctica: un enfoque dinámico" hacen referencia a la misma cuando explican que los procedimientos de seguridad deberían servir para saber cómo, cuándo y qué usuario accede a una parte de la información. Por lo tanto, estos procedimientos sirven para controlar dicho acceso lógico, y en caso de que no sea el usuario adecuado para la información, el sistema bloqueará la misma. Para ello, se deberán incluir barreras y controles que protejan el acceso a los datos por parte de terceras personas que no tengan la autorización necesaria.

Los puntos clave u objetivos a tener en cuenta, según Piattini y Del Peso Navarro, al hablar de seguridad lógica, pueden resumirse en los siguientes:

- En caso de problemas en la transmisión debe de haber un proceso de emergencia con el fin de que la información pueda llegar hasta el destinatario.
- Comprobar que los empleados que usen dichos archivos y programas puedan estar trabajando sin necesidad de una supervisión y que a la vez no sean capaces de cambiar o modificar los archivos y programas que no les corresponden como empleados.
- La información recibida por el destinatario, tiene que ser la misma que la que fue enviada desde el origen.
- Limitar el acceso a los archivos y programas de la entidad.
- Sostener que los empleados que están utilizando los archivos, programas y los datos están siendo utilizados en el procedimiento correcto y no por otros.
- Toda la información transferida solo puede ser recibida por el destinario real, y no a terceros, ya que esto sería un grave problema en la entidad.

Deben de existir diferentes caminos de transmisión entre diferentes puntos.
El fraude y los accesos no autorizados son ejemplos de incumplimiento lógico malicioso, y aunque el problema pudo haber sido introducido accidentalmente en un ordenador, su concepción original es maliciosa.

Las casusas de la falta de seguridad lógica son, entre toras, las siguientes:

- Los virus
- Programas no testeados
- Errores de usuario
- Error del operador
- Mal uso del ordenador
- Fraude informático
- Investigación de accesos no autorizados internos
- Acceso no autorizados externos

Uno de los problemas con cualquier violación de la seguridad lógica informática es que el daño es invisible y su extensión es desconocida. El coste de investigación es muy probable que sea alto.

Esto es particularmente cierto con las infecciones de virus ya que existen infecciones maliciosas que pueden borrar (o, peor aún, corromper) los datos de todo un disco. El virus puede ser transferido a cualquier otra unidad que entra en contacto con un PC infectado sin que nos demos cuenta. Cada PC que entra en contacto con esa unidad infectada tiene que comprobarse, y cada otra unidad adicional que se haya cargado en cualquiera de esos ordenadores infectados, también tendría que comprobarse, y después todas las unidades que hayan sido cargadas en esos ordenadores, y así sucesivamente. Pueden llegar a ser miles de ordenadores y unidades las que tienen que ser revisadas en una organización grande. Y eso sin tener en cuenta que además los virus también pueden ser transmitidos a otros ordenadores a través de la red.

C.CONTROLES DE ACCESO

Los controles de acceso son una herramienta totalmente necesaria y básica para tener un mínimo de seguridad lógica en la entidad. Además son de una gran ayuda ya que protegen a nuestro sistema respecto a modificaciones no consentidas, mantienen la integridad de nuestra información, protegen las aplicaciones que estamos utilizando y protegen la información respecto a empleados que no tienen el acceso necesario para ello. Al respecto, el National Institute for Standars and Technology (NIST) ha resumido los siguientes estándares de seguridad que se refieren a los requisitos mínimos de seguridad en cualquier sistema:

- Identificación y autentificación

Es la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

Se denomina Identificación al momento en que el usuario se da a conocer en el sistema; y Autenticación a la verificación que realiza el sistema sobre esta identificación.

- Roles

El acceso a la información también puede controlarse a través de la función o rol del usuario que requiere dicho acceso.

- Transacciones

También pueden implementarse controles a través de las transacciones.

- Limitaciones a los servicios

Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema.

- Modalidad de acceso

Se refiere al modo de acceso que se permite al usuario sobre los recursos y a la información. Esta modalidad puede ser:

- Lectura: el usuario puede únicamente leer o visualizar la información pero no puede alterarla. Debe considerarse que la información puede ser copiada o impresa.
- Escritura: este tipo de acceso permite agregar datos, modificar o borrar información.
- Ejecución: este acceso otorga al usuario el privilegio de ejecutar programas.
- Borrado: permite al usuario eliminar recursos del sistema El borrado es considerado una forma de modificación.
- Creación: permite al usuario crear nuevos archivos, registros o campos.
- Búsqueda: permite listar los archivos de un directorio determinado.

1. CONTROLES DE ACCESOS INTERNOS

Algunos de los controles de acceso internos que se pueden imponer son:

- Palabras claves (passwords): Una contraseña o password es una serie secreta de caracteres que permite a un usuario tener acceso a un archivo, a un ordenador, o a un programa, cada usuario debe incorporar su contraseña antes de que el ordenador responda a los comandos. Las contraseñas ayudan a asegurar que los usuarios desautorizados no tengan acceso al ordenador. Idealmente, la contraseña debe ser algo que nadie pueda adivinar. En la práctica, la mayoría de la gente elige una contraseña que sea fácil de recordar, por ejemplo su nombre o sus iniciales con lo que se ve disminuida la utilidad de esta técnica.

- Encriptación: La información encriptada solamente puede ser desencriptada por quienes posean la clave apropiada. La encriptación puede proveer de una potente medida de control de acceso.

- Listas de control de accesos: Se refiere a un registro donde se encuentran los nombres de los usuarios que obtuvieron el permiso de acceso a un determinado recurso del sistema, así como la modalidad de acceso permitido. Este tipo de listas varían considerablemente en su capacidad y flexibilidad.

- Límites sobre la interface de usuario: Esto límites, generalmente, son utilizados en conjunto con las listas de control de accesos y restringen a los usuarios a funciones específicas. Básicamente pueden ser de tres tipos: menús, vistas sobre la base de datos y límites físicos sobre la interface de usuario. Por ejemplo los cajeros automáticos donde el usuario sólo puede ejecutar ciertas funciones presionando teclas específicas.

- Etiquetas de seguridad: Consiste en designaciones otorgadas a los recursos (como por ejemplo un archivo) que pueden utilizarse para varios propósitos como control de accesos, especificación de medidas de protección, etc. Estas etiquetas no son modificables

2. CONTROLES DE ACCESOS EXTERNOS

- Dispositivos de control de puertos: Estos dispositivos sirven para controlar todas las acciones de los dispositivos que se conecten a los distintos puertos, permitiendo y restringiendo acciones. el administrador puede seleccionar para distintos tipos de dispositivos externos las acciones que se desean restringir en cada PC. Las acciones que se pueden establecer sobre los diferentes tipos de dispositivos son: Bloquear todas las acciones del tipo de dispositivo seleccionado, permitir sólo la lectura en el tipo de dispositivo seleccionado o permitir operaciones tanto de lectura como de escritura.

- Firewalls o puertas de seguridad: Un cortafuegos es la parte de un sistema informático o una red informática que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo

comunicaciones autorizadas, es decir, permiten que los usuarios internos se conecten a la red exterior al mismo tiempo que previenen la intromisión de atacantes o virus a los sistemas de la organización

- Acceso de personal contratado o consultores: Debido a que este tipo de personal en general presta servicios temporarios, debe ponerse especial consideración en la política y administración de sus perfiles de acceso.

- Acceso público: Para los sistemas de información consultados por el público en general, o los utilizados para distribuir o recibir información computarizada deben tenerse en cuenta medidas especiales de seguridad, ya que se incrementa el riesgo y se dificulta su administración. Debe considerarse para estos casos de sistemas públicos, que un ataque externo o interno puede acarrear un impacto negativo en la imagen de la organización.

D.ADMINISTRACIÓN DE LA SEGURIDAD

Una vez establecidos los controles de acceso sobre los sistemas y la aplicación, es necesario realizar una eficiente administración de estas medidas de seguridad lógica, lo que involucra la implementación, seguimientos, pruebas y modificaciones sobre los accesos de los usuarios de los sistemas.

La política de seguridad que se desarrolle respecto a la seguridad lógica debe guiar a las decisiones referidas a la determinación de los controles de accesos y especificando las consideraciones necesarias para el establecimiento de perfiles de usuarios.

E.SEGURIDAD LÓGICA EN LA MUNICIPALIDAD DE LUJÁN DE CUYO

1. CONTROLES DE ACCESO

En relación a los controles de acceso internos cada agente municipal que trabaja en el área de informática tiene una password de acceso o encendido a su PC de trabajo. Los agentes municipales en general tienen la posibilidad de tener este tipo de password de acceso a su PC pero, como bien se menciona, es sólo una opción generando que no exista un control estricto de esta situación. Asimismo el sistema Municipal (MAJOR) que posee múltiples módulos de gestión (entre ellos: Tesorería, Ingresos Públicos, Contrataciones, Contabilidad, Gestión de Documentos, Mesa de Entradas, Solicitante, etc.) tiene diversos niveles de acceso asignados a cada agente municipal previo pedido mediante nota dirigida a un responsable específico del sector quien lleva un listado de control de niveles y modalidades de accesos. A su vez el personal posee diversas modalidades de acceso: Lectura, escritura, ejecución, consulta o búsqueda y borrado otorgados por el responsable mencionado anteriormente.

Con respecto a los controles de acceso externos de acuerdo a lo expresado por el agente entrevistado existen Firewalls orientados a proteger el software no así el hardware. Aunque no existen dispositivos que controlen las acciones de los dispositivos que se conecten a los distintos puertos, no se poseen PCS de acceso público que incrementen el riesgo asociado a este tipo de accesos.

2. ADMINISTRACIÓN DE SEGURIDAD

Actualmente existe un módulo informático que sirve para realizar controles y auditorías con respecto memorias de usos y accesos a la base de datos lo que implica que existen políticas de implementación, seguimientos, pruebas y modificaciones sobre los accesos de los usuarios a los sistemas debido a que el sistema fue diseñado para establecer alarmas y controlar la evolución con datos actualizados en tiempo real. Asimismo ante el pedido de áreas jerárquicas superiores motivado por una sospecha relacionada con la modificación, adulteración o borrado de cierta información, se efectúa un control de accesos histórico que brinda un detalle exhaustivo de los movimientos específicos realizados por dicha persona.

Se auditan periódicamente la calidad de los datos contenidos en las bases de datos y archivos digitales de la organización ya que existe un área de auditoría interna que a través de las revisiones de los distintos tipos de sectores efectúa el control de la base de datos que surge de cada módulo del sistema.

En resumen en este capítulo se pone de manifiesto la importancia de la seguridad lógica en forma complementaria a la física resultando ambas igual de determinantes a la hora de establecer un eficiente plan de seguridad global. Se puede evidenciar cómo los controles de acceso lógicos influyen sobre el impacto de las vulnerabilidades a las que los sistemas informáticos se encuentran expuestos, disminuyendo dichos riesgos a niveles aceptables si en forma conjunta, ejercemos una correcta y eficiente administración de estas medidas de seguridad.

CAPÍTULO IV:
DELITOS INFORMÁTICOS

En este capítulo se comienza abordando una aproximación conceptual del delito informático junto con sus elementos y características, luego se describen los distintos grupos de conductas delictivas que existen y se manifiestan y plasman en las diferentes tipologías de conductas nocivas que se pueden cometer a través de sistemas. Posteriormente se expone el encuadre legal que le brinda la legislación argentina a este tipo de delitos, y finaliza con la enumeración de este tipo de conductas vividas a lo largo de la historia por la institución bajo análisis.

A. APROXIMACIÓN CONCEPTUAL, ELEMENTOS Y CARACTERÍSTICAS

Se considera que no existe una definición formal y universal de delito informático pero se han formulado conceptos respondiendo a realidades nacionales concretas.

No resulta fácil definir delito informático, ni siquiera la doctrina encuentra un concepto unitario para definirlo. Según Tiedemann, (Tiedemann, citado por Molina, 1988, p. 307) los delitos informáticos, aluden a todos los actos antijurídicos según la ley penal vigente, realizados con el empleo de un equipo automático de datos. (Morabito, 2014)

Menéndez Mato, J.C. y Gayo Santa Cecilia, en su obra Derecho e Informática: Ética y Legislación cita a Landaverde y a M. L., Soto, J. G. & Torres, J. M. (2000), los cuales coinciden al decir que para hablar de los delitos informáticos se requiere, en una primera instancia definir qué es un delito, y luego qué es la informática. Como sabemos un delito es un acto u omisión sancionado por las leyes penales y tiene los siguientes elementos:

•Es un acto humano (acción u omisión).

•Ese acto humano debe ser antijurídico, debe lesionar o poner en peligro un interés jurídicamente protegido.

•Debe ser un acto típico. (Definido por la ley)

•Actor debe ser culpable, imputado a dolo o culpa.

•La ejecución u omisión del acto debe estar sancionada por una pena.

De una forma genérica, flexible y bajo una terminología lo más sutil y pragmática posible, el delito informático se conceptualiza como todo acto, comportamiento y/o conducta indebida, ilícita e ilegal que encuadra en figuras tradicionales ya conocidas como robo, hurto, fraude, falsificación, perjuicio, estafa y sabotaje que propicie ser razonado como criminal, orientado a la alteración y/o

destrucción de cualquier sistema de información o alguno de sus componentes que la integren, generando como producto final un daño lesivo al tratamiento de la información, siempre que involucre a la informática de por medio para cometer la ilegalidad.

Algunas características son del delito informático son:

• Conductas criminales de cuello blanco.

• Son acciones de oportunidad.

• Provocan serias pérdidas económicas.

• Presentan grandes dificultades para su comprobación.

1. TIPOS DE DELITOS Y SUS CARACTERÍSTICAS

Según Ministerio del Interior de España (2013) los delitos se agrupan de la siguiente manera:

Grupo de conducta Delictiva	**Características generales**
Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos	Se incluye el acceso ilícito a sistemas informáticos; la interceptación ilícita de datos informáticos; la interferencia en el sistema mediante la introducción, transmisión, provocación de daños, borrado, alteración o supresión de estos; y el abuso de dispositivos que facilitan la ejecución de delitos.
Fraudes informáticos	Incluye la falsificación informática que produzca la alteración, borrado o supresión de datos informáticos que ocasionen datos no auténticos.
Delitos relacionados con el contenido	Este grupo aborda los delitos relacionados con la pornografía infantil.
Delitos relacionados con infracciones de la propiedad intelectual y derechos afines	En orden del cumplimiento del Convenio sobre la Ciberdelincuencia, los países firmantes deben considerar la tipificación de estas conductas como delitos, en su derecho interno
Delitos relacionados con el robo de servicios	Este grupo comprende las acciones indebidas relacionadas con el hurto del tiempo del computador; la apropiación de informaciones residuales (scavenging); el parasitismo informático (piggybacking) y la suplantación de personalidad (impersonation).

Delitos relacionados con el espionaje informático y el robo o hurto de software.	Relaciona lo comprendido con respecto a fuga de datos (data leakage) y la reproducción no autorizada de programas informáticos de protección legal.

B. CONDUCTAS NOCIVAS QUE SE COMETEN A TRAVÉS DE SISTEMAS

A continuación según la cátedra de Auditoría Operativa de la Facultad de Ciencias Económicas de la Universidad Nacional de Cuyo las conductas comportamentales integrantes de esta clase de acciones indebidas e ilícitas son:

1. MALWARE

Malware es la abreviatura de "Malicious software" (software malicioso), término que engloba a todo tipo de programa o código de computadora cuya función es dañar un sistema o causar un mal funcionamiento. Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o Sistema de información sin el consentimiento de su propietario. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de software hostil, intrusivo o molesto.

2. SPYWARE

Son programas creados para recopilar información sobre las actividades realizadas por un usuario y distribuirla a terceros interesados. Algunos de los datos que recogen son las visitas que realiza el usuario y direcciones a las que luego se envía. La mayoría de los programas spyware son instalados como troyanos junto a software deseable bajado de Internet, aunque esto no significa que todo el software que muestra anuncios o realiza un seguimiento en línea, sea maligno.

Otro tipo de spyware realiza modificaciones en el equipo que pueden resultar molestas y hacer que su funcionamiento sea más lento o que se bloquee.

El spyware y el software no deseado pueden entrar en el equipo de varias maneras. Un caso común es cuando se instala de manera encubierta durante la instalación de otro software que usted desea instalar, como software de uso compartido de archivos de música o video.

Siempre que se instale algo en el equipo, hay que asegurarse de leer con detenimiento toda la información, incluido el contrato de licencia y la declaración de privacidad. En ocasiones, la inclusión de software no deseado en la instalación de un determinado programa está documentada, aunque sea al final del contrato de licencia o de la declaración de privacidad.

3. ADWARE

"Advertising-Supported software" (Programa Apoyado con Propaganda) es cualquier programa

que automáticamente muestra publicidad web al usuario durante su instalación o durante su uso para generar lucro a sus autores. Éstos suelen venir incluidos en Programas Shareware (Software con modalidad de distribución gratuita), de manera que al aceptar los términos legales durante la instalación de éstos programas, estamos consintiendo su ejecución en nuestros equipos y afirmando que estamos informados de ello.

4. VIRUS

Un virus informático es un malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario; es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos, puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.

Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos o realizar acciones maliciosas como por ejemplo: borrar archivos.

Estos se propagan más fácilmente mediante datos adjuntos incluidos en mensajes de correo electrónico o de mensajería instantánea. Por este motivo es fundamental no abrir nunca los datos adjuntos de correo electrónico a menos que sepa de quién procede y los esté esperando. Un virus necesita de la intervención del usuario para propagarse mientras que un gusano se propaga automáticamente.

5. GUSANOS

Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede degenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

6. BOMBA LÓGICA O CRONOLÓGICA

Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo

después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba

7. ACCESO NO AUTORIZADO A SERVICIOS Y SISTEMAS INFORMÁTICOS

Este acceso se puede dar por motivos diversos, desde la simple curiosidad, como en el caso de muchos piratas informáticos hasta el sabotaje o espionaje informático.

8. SUPLANTACIÓN DE IDENTIDAD

Puede ser entendida como la suplantación de personalidad fingiendo ser una persona que no es imitándola e inclusive remedándola. El caso más común es el robo de tarjetas de crédito y de cajeros automáticos. Los autores del delito se hacen pasar por empleados de la central de tarjetas de crédito, llamando telefónicamente al titular para solicitarle que con el objeto de anular la posibilidad de utilización fraudulenta de la tarjeta robada le revele su clave secreta o personal.

En la actualidad con el desarrollo de las redes sociales en Internet, una nueva modalidad es la creación de páginas o usuarios suplantando a otra persona.

9. PHISHING

Los ataques de estafa a través de Internet por el método “phishing”, que significa “pesca” en el argot informático, se han ido incrementando. El sistema más utilizado por los cyber-estafadores es el envío de correos electrónicos con falsos remitentes, como por ejemplo de entidades financieras, de forma tal que las víctimas cliquearan en un link y de esa forma podían obtener información personal.

Pero ya se habla de una nueva generación de phishing, demuestra cómo es posible realizar ataques phishing en servidores seguros de entidades bancarias, aun cuando el usuario visualice que la URL comienza por https:// seguido del nombre de la entidad y que el icono del candado que aparece en la parte inferior del navegador certifique que se encuentra en el servidor seguro del banco, lo que constituían hasta el momento las recomendaciones que se hacían para acceder de forma segura a la banca electrónica. Como podemos ver esto se ha vuelto inseguro y el Pharming es la confirmación de esta afirmación. Algunos Derivados del Phishing son el “**Scam”** el cual tiene como objetivo obtener datos confidenciales de usuarios, para acceder a sus cuentas bancarias. A través de envíos masivos de correos electrónicos o la publicación de anuncios en webs, en los que se ofrecen empleos muy bien remunerados cuando el usuario acepta la oferta de trabajo, se le solicita que facilite datos de sus cuentas bancarias, a través de un e-mail o accediendo a una web, para ingresarle los supuestos beneficios, el **Smishing** en

donde el ataque se realiza a través de los mensajes a teléfonos móviles, el estafador suplanta la identidad de una entidad de confianza para solicitar al usuario que facilite sus datos, a través de otro SMS o accediendo a una página web falsa, idéntica a la de la entidad en cuestión, el **Spear Phishing** en el que, en lugar de realizar un envío masivo de correos electrónicos, se envían correos con mayor grado de personalización, a destinatarios concretos, consiguiendo que los mensajes resulten más creíbles que los del phishing tradicional, el **Vishing** en el cual también se persigue la obtención de datos confidenciales de los usuarios, pero a través de la telefonía IP y el **Scavenging** a través del cual se apropian de informaciones residuales, la que consiste en la obtención de información a partir de lo que desechan los usuarios legítimos de un sistema informático.

10. RANSOMWARE

Un ransomware o "secuestro de datos" en español, es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo infectado, y pide un rescate a cambio de quitar esta restricción. Algunos tipos de ransomware cifran los archivos del sistema operativo inutilizando el dispositivo y coaccionando al usuario a pagar el rescate.

11. UTILIZACIÓN DE BACKDOORS

Las puertas traseras son trozos de código en un programa que permiten a quien las conoce saltarse los métodos usuales de autentificación para realizar ciertas tareas.

Habitualmente son insertados por los programadores del sistema para agilizar la tarea de probar código durante la fase de desarrollo". Esta situación se convierte en una falla de seguridad si se mantiene, involuntaria o intencionalmente, una vez terminado el producto ya que cualquiera que conozca el agujero o lo encuentre en su código podrá saltarse los mecanismos de control normales

12. UTILIZACIÓN DE EXPLOITS

Es muy frecuente ingresar a un sistema explotando agujeros en los algoritmos de encriptación utilizados, en la administración de las claves por parte la empresa, o simplemente encontrando un error en los programas utilizados. Los programas para explotar estos "agujeros" reciben el nombre de Exploits y lo que realizan es aprovechar la debilidad, fallo o error hallado en el sistema (hardware o software) para ingresar al mismo. Nuevos Exploits (explotando nuevos errores en los sistemas) se publican cada día por lo que mantenerse informado de los mismos y de las herramientas para combatirlos es de vital importancia.

C. LEGISLACIÓN NACIONAL

Antes de la sanción de la ley 26.388 la falta de tipificación penal de muchas conductas delictivas producía que las mismas quedaran impunes y no pudieran ser sancionadas penalmente, con la mencionada ley, la cual es una modificación al Código Penal, se sustituyeron e incorporaron algunas figuras típicas con el fin de regular a las nuevas tecnologías utilizadas como medio para cometer delitos. Las figuras contempladas son:

- Daño informático.
- Fraude informático.
- Alteración de pruebas.
- Financiación, distribución, etc. de pornografía infantil por medios informáticos.
- Delitos contra la privacidad.
- Delitos contra la seguridad pública.
- Falsificación de documentos electrónicos.

A su vez en su art. 1 amplía los conceptos de "documento", "firma", "suscripción", "instrumento privado" y "certificado" incluyendo en los mismos a los soportes magnéticos o de otro tipo informático, la firma digital y los documentos y certificados digitales.

Esta ley también modificó el artículo 128 del Código Penal condenando al que "produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales…"

Por lo anteriormente expuesto es que nuestra legislación regula Comercial y Penalmente las conductas ilícitas relacionadas con la informática, pero que aún no contemplan en sí los delitos informáticos por lo tanto sería necesario y muy importante que la ley contemplara este tipo de delitos condenando los accesos ilegales a las redes como a sus medios de transmisión y prohibiendo toda clase de acceso no autorizado a un sistema informático

Otras leyes relacionadas con la seguridad informática son: La Ley 24.766, llamada de confidencialidad de datos, la cual tutela la información que importe un secreto comercial. La Ley 25.326, llamada de hábeas data, la misma tutela la información de carácter personal almacenada en archivo de datos. La Ley 11.723, de propiedad intelectual, que tutela las obras de computación fuente y objeto. La Ley 22.362 de marcas y la Ley 24.481 de patentes.

D.DELITOS INFORMÁTICOS Y CONDUCTAS NOCIVAS COMETIDAS EN LA MUNICIPALIDAD DE LUJÁN DE CUYO

De acuerdo a la entrevista realizada, ante una sospecha de ingreso no autorizado al sistema Municipal o siendo un ingreso autorizado donde existen sospechas relacionadas con la integridad de los datos se realiza la auditoría correspondiente, habiéndose detectado en ciertos momentos pasados, casos

de delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos como también fraudes informáticos (falsificación informática que produjo la alteración, borrado o supresión de datos informáticos ocasionando datos no auténticos).

Con respecto a las conductas nocivas cometidas a través de sistemas hay registros de Virus en la Policía Vial que afectaron a 10 máquinas, esta situación se solucionó con el cambio del sistema operativo. También se detectó un ransomware el cual también pudo detenerse. Asimismo se poseen registros de blackdoors remotas y exploits los cuales fueron muy difíciles de detener ya que según lo informado llegaron a penetrar a través de la Deep web.

Recapitulando es importante mencionar que una vez que se definen los delitos informáticos detectando sus elementos integrantes y sus características junto con su manifestación a través de las conductas nocivas enumeradas en este capítulo estamos en condiciones de darle un tratamiento adecuado a estos aspectos teniendo en cuenta las medidas de seguridad a implementar, haciendo especial énfasis nuevamente en el tratamiento del factor humano a través de la sanción de distintas leyes que penan este tipo de conductas.

CAPÍTULO V:
COMUNICACIONES Y SISTEMAS

En este capítulo se desarrollarán aquellos conceptos referidos a las comunicaciones abordando las redes informáticas y dentro de estas a internet como recurso y herramienta primordial de trabajo y comunicación, resultando ser el principal medio para la comisión de ataques informáticos y por lo tanto en donde se deben aplicar mayores esfuerzos para promover medidas de seguridad. A su vez como integrante del aspecto comunicacional se analizan los sistemas de gestión, los cuales resultan imprescindibles para aplicar y manejar las políticas y los procedimientos de una organización de manera integrada y eficaz. Se finaliza con el análisis e impacto de ambos aspectos en la Municipalidad de Luján de Cuyo.

A.CONCEPTO Y OBJETIVOS DE REDES INFORMÁTICAS

Según Raffino (2019) se entiende por redes informáticas a un número de sistemas informáticos conectados entre sí mediante una serie de dispositivos alámbricos o inalámbricos, gracias a los cuales pueden compartir información en paquetes de datos, transmitidos mediante impulsos eléctricos, ondas electromagnéticas o cualquier otro medio físico.

Las redes informáticas no son distintas en su lógica de intercambio de los demás procesos de comunicación conocidos: cuentan con un emisor, un receptor y un mensaje, así como un medio a través del cual transmitirlo y una serie de códigos o protocolos para garantizar su comprensión. Claro que en este caso, quienes envían y reciben mensajes son sistemas computacionales automatizados.

Cuando se dispone de computadores en red, es posible crear una comunicación interna, compartir un punto de acceso a Internet o la administración de periféricos (impresoras, escáneres, etc.), así como el envío veloz de datos y archivos sin necesidad de dispositivos de almacenamiento secundario. Esto se logra gracias a una serie de estándares de comunicación, que “traducen” a un mismo idioma los procesos de los diversos computadores (el más común de ellos es el TCP/IP).

Uno de los objetivos de las redes es hacer que todos los programas, datos y equipos estén disponibles para cualquier usuario de la red que así lo solicite, sin importar la localización física del recurso y del usuario. Otro objetivo consiste en proporcionar una alta fiabilidad, al contar con fuentes alternativas de suministro. La presencia de múltiples CPUs significa que si una de ellas deja de funcionar, las otras pueden ser capaces de encargarse de su trabajo, aunque el rendimiento global sea menor. Por último podemos mencionar el objetivo del ahorro económico ya que las computadoras pequeñas tienen una mejor relación costo/rendimiento, comparada con la ofrecida por las máquinas

grandes. Estas son, a grandes rasgos, diez veces más rápidas que el más rápido de los microprocesadores, pero su costo es miles de veces mayor. Este desequilibrio ha ocasionado que muchos diseñadores construyan sistemas constituidos por poderosos ordenadores personales, uno por usuario y con los datos guardados en una o más máquinas que funcionan como servidor de archivo compartido.

Este objetivo conduce al concepto de redes con varias computadoras en el mismo edificio las cuales se le denomina LAN, en contraste con lo extenso de una WAN.

B.ESTRUCTURA BÁSICA DE LA WEB

La estructura básica de la World Wide Web (WWW) consiste en una red informática mundial accesible a través de Internet. Está formada por páginas web interconectadas que ofrecen diversos tipos de contenido textual y multimedia. La World Wide Web se basa en hipertextos, es decir, archivos de texto (páginas) en los que se pueden insertar hipervínculos o enlaces que conducen a los usuarios de una página web a otra, o a otro punto de esa misma página. El tipo más común de datos transportado a través de HTTP es HTML (HiperText Markup Language). Además de incluir directrices para la "compresión" de textos, también tiene directrices que proporcionan capacidades como las de enlaces de hipertexto y la carga de imágenes en línea. Los recursos hiperenlazados y los archivos de imágenes en línea están identificados con los URL intercalados dentro del documento HTML.

1. INTERNET

Como se mencionó anteriormente la estructura básica de la World Wide Web es accesible a través de Internet. Internet es una red que conecta infinitas redes entre sí, por lo cual se la conoce como la red de redes debido a que el progreso de la comunicación digital tiene su base en el uso de la misma y las nuevas tecnologías.

Surgió en los años 80 como un proyecto militar, en pocos años se fue extendiendo y llegando a los hogares superando su desarrollo ampliamente cualquier previsión y constituyendo una verdadera revolución en la sociedad moderna. A su vez se transformó en un pilar de las comunicaciones, el entretenimiento y el comercio en todos los rincones del planeta.

Los servicios y protocolos disponibles en la red de redes son el acceso remoto a computadoras conocido como Telnet, el sistema de transferencia de archivos FTP, el correo electrónico (POP y SMTP), el intercambio de archivos P2P y las conversaciones online o chats. Los servicios y recursos de Internet (Gopher, News, Archie, WWW, etc.) son accesibles de diversas formas, principalmente tres: por Telnet, por e–mail, y por un programa cliente. A través de Telnet o e–mail, el servicio presenta una interface ANSI (sin gráficos), sólo con caracteres alfanuméricos. Con un programa cliente, la gestión es más sencilla, visual y agradable, como sucede en la WWW donde se presentan cada una de las páginas en

formato gráfico.

2. PROBLEMAS DE SEGURIDAD EN LOS SERVIDORES WWW

Hoy en día las conexiones a servidores web son sin duda las más extendidas entre usuarios de Internet. A continuación se mencionarán los problemas de seguridad relacionados con el protocolo HTTP divididos en tres grandes grupos en función a los datos a los que pueden afectar:

• Seguridad en el servidor: es necesario garantizar que la información almacenada en la máquina servidora no pueda ser modificada sin autorización, que permanezca disponible y que sólo pueda ser accedida por los usuarios a los que les esté legítimamente permitido.

• Seguridad en la red: cuando un usuario conecta a un servidor web se produce un intercambio de información entre ambos; es vital garantizar que los datos que recibe el cliente desde el servidor sean los mismos que se están enviando (esto es, que no sufran modificaciones de terceros), y también garantizar que la información que el usuario envía hacia el servidor no sea capturada, destruida o modificada por un atacante.

• Seguridad en el cliente: es necesario garantizar al usuario que descarga páginas de un servidor no va a perjudicar a la seguridad de su equipo. Se deben evitar Applets maliciosos, programas con virus o simples cuelgues al acceder a las páginas de la organización. Ante hechos de esta especie seguramente la persona dejará de visitarlas, con la consecuente pérdida de imagen (y posiblemente un cliente) de esa entidad.

C. SISTEMAS DE GESTIÓN

Los sistemas de gestión son programas diseñados para manejar las políticas y los procedimientos de una organización de manera eficaz. Este mecanismo de gestión documenta cada uno de los procesos de la empresa. A su vez estos sistemas en el ámbito de la administración pública comprenden el conjunto de herramientas integradas necesarias para lograr el control efectivo sobre la facturación, el aumento de la recaudación basado en una mejor respuesta en el pago voluntario de los tributos, un mejor seguimiento de los contribuyentes, información de gestión confiable, la disminución de los costos administrativos y una simple y completa gestión operativa logrando la disminución progresiva de la evasión impositiva y la reducción de los costos administrativos, basándose en estadísticas de facturación y recaudación precisas y confiables. En definitiva, un sistema de gestión eficiente permite, entre otras cosas, aumentar la base de contribuyentes que pagan, lograr una distribución equitativa de la carga tributaria y mayores recursos para el Municipio.

Los sistemas de gestión pueden ser a medida o estándar o enlatados. Los primeros se llaman

justamente “a medida” porque el sistema o software se adapta a los procesos de gestión que la empresa ya tiene consolidados. En el desarrollo de un sistema a medida, siempre se realiza una primera etapa de análisis, en la cual se estudian los procesos de la empresa, se determina como intervendrá el nuevo sistema en estos procesos y siempre es un muy buen momento para repensar los procesos y mejorarlos. Es el software el que se adapta a la empresa.

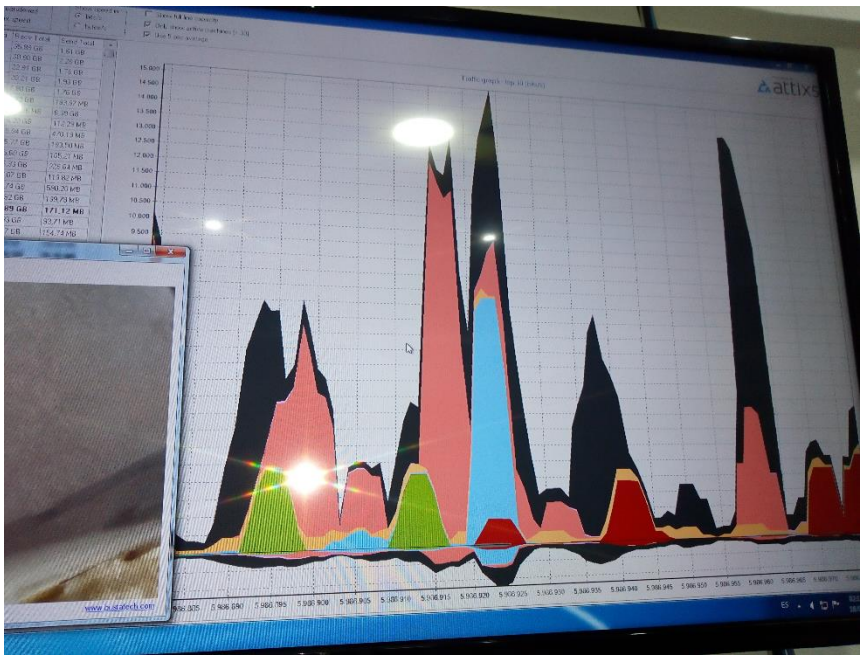
El software estándar o "enlatado", es un software genérico, que resuelve múltiples necesidades, y la empresa probablemente sólo empleará algunas. En general, es un software que no se adapta completamente al vocabulario, necesidades y funciones que necesita la empresa.

D. MUNICIPALIDAD DE LUJÁN DE CUYO

1. SERVICIO DE INTERNET Y SEGURIDAD DEL MISMO

Con respecto a las medidas de seguridad implementadas relacionadas con acceso a las redes e internet se encuentran bloqueadas las páginas de ocio (redes sociales, YouTube, etc.) para la mayoría de los agentes municipales con el fin de asegurar un correcto uso de la herramienta laboral. Asimismo se lleva un registro de accesos a internet a través de una curva estadística (Imagen 9) en donde si se detecta un pico y no proviene de niveles gerenciales se pide la justificación pertinente al superior jerárquico del agente municipal en cuestión. Si el encargado no está en conocimiento de esta situación se procede a restringir la velocidad y en ocasiones el acceso a internet.

Imagen 9: Curva estadística uso internet



En cuanto al servicio de internet que actualmente posee el Municipio se pudo relevar la siguiente

información a través de la observación del respectivo expediente: A mediados de 2018 el Municipio inició el procedimiento administrativo para proceder a la contratación del servicio de Internet, en donde el área de Informática y Comunicaciones expresa que el motivo de dicha solicitud es la ampliación del ancho de banda debido a que es un servicio fundamental para:

- Mantener comunicados con redistribución de señal a las Delegaciones, dependencias externas y oficinas internas.
- Trámites internos que deben ser resueltos a través de la Web y dirigidos hacia otras instituciones u organismos de control
- Medio de comunicación utilizado por las empresas proveedoras de servicios informáticos y software de gestión Municipal que implican mantener videoconferencias y seguimiento de requerimientos, capacitación, implementaciones y puesta a punto de los sistemas.
- Armado de vínculos VPN (Red privada virtual) para mantener en línea los servicios de asistencia remota y accesos desde las dependencias externas hacia el Municipio utilizando los sistemas de gestión, con transacciones ejecutadas en tiempo real.
- Servicios de sistemas de cobranzas y de autogestión del contribuyente
- Servicios de sistemas de reclamos que interactúan con el contribuyente
- Servicios de acceso a la página institucional
- Servicios de acceso a los sistemas de turnos
- Servicio de correo institucional, redes sociales, WhatsApp, etc.
- Servicio de trabajo colaborativo por intermedio de Office365
- Servicio de recepción de documentación externa proveniente de contribuyentes, instituciones y organismos de control.
- Servicios de geo localización de aparatos celulares de inspectores y sus recorridos
- Funcionamiento del sistema de información geográfica (GIS): Se necesita un ancho de banda suficiente para soportar el servicio de información catastral de construcciones del departamento. Para el área creada a tal efecto, el personal abocado a la actualización y mejora de datos poseen licencias multiusuarios en el área GIS, utilizando internet, hoy no se puede ejecutar con la funcionalidad y agilidad requerida porque el servicio es insuficiente.
- El sistema de Obras Privadas Online se encuentra en condiciones para llevarlo a la etapa de producción en el mes de septiembre. No se puede utilizar el sistema por el faltante de ancho de banda, por lo tanto provoca atrasos a la etapa de pruebas, corrección de errores, evaluación y puesta en marcha.

Luego en su último párrafo menciona que actualmente se cuenta con 300 Mb de ancho de banda (insuficiente para mantener todo el servicio activo), en base al consumo evaluado es que se necesita aumentar la capacidad a 120 mb concentrando la prioridad en el DataCenter, Edificio central, edificio de hacienda, salón Taboada, dándole énfasis a esos sectores, a la correspondiente distribución en las

dependencias externas y delegaciones.

En función a lo anteriormente expuesto se procede al llamado a licitación pública a través del expediente 8870/2018. En el pliego de especificaciones técnicas se describen los requerimientos a cumplir en cuanto a seguridad:

En conjunto con el Servicio de Internet solicitado, deberá brindarse el servicio que se detalla a continuación:

* Mesa de ayuda y Monitoreo 7x24.

* Soporte y mantenimiento 7x24.

***** Operación remota en forma segura.

* Reportes de gestión mensuales.

* Mantenimiento preventivo y correctivo.

* Análisis de eventos y logs.

*Respuesta ante incidentes (Ejemplo: Ataques externos, actividades sospechosas, propagación de virus, malware, Spyware, etc.) a través del SOC (Security Operation Center) en modalidad 7x24.

* Se deberá proveer un sistema de reportes e informes adecuados y en tiempo real.

Para lograr este propósito el sistema deberá reportar:

• Servicios: (gráficas de uso del servicio, tráfico).

• Fallas: listado de fallas, fecha y hora de inicio, fecha y hora de finalización, servicio afectado, fecha y hora de notificación de la falla, motivo de la falla, observación.

• Utilización de línea: porcentaje de uso de la línea en Mbps, frames, etc., tanto de tráfico entrante como saliente comparado con el ancho de banda total disponible.

• Disponibilidad: % de satisfacción desagregado por servicio.

• Otros

Dicho sistema deberá mostrar en modo gráfico los parámetros que correspondan, en escala mensual, semanal y diaria.

VPN: Las redes privadas virtuales (VPN por sus siglas en inglés) permitirán crear un túnel de comunicación seguro (L2TP, PPTP Y SSL), a través de una red pública (Ejemplo Internet). Deberá contar con soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site) y VPNs SSL, deberá soportar los algoritmos de cifrado: AES, DES, 3DES; longitudes de llave para AES de 128, 192 y 256 bits; algoritmos de integridad: MD5, SHA-1 y SHA256. Deberá proveer soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet. El equipamiento ofrecido deberá soportar al menos 10 conexiones VPN. Este servicio permitirá compartir información entre diferentes sitios del Municipio o permitir el acceso de usuarios remotos de manera segura y protegida

Filtrado de URLs (URL Filtering): Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 75 categorías y por lo menos 54 millones de sitios web en la base de datos. Debe poder categorizar

contenido Web requerido mediante IPv4 o IPv6.

Filtrado de Contenido: El sistema de filtrado de contenido deberá restringir y controlar el acceso a Internet. De esta manera se podrá optimizar el ancho de banda priorizando el uso de herramientas necesarias (correo electrónico, ERP, etc.) y evitar el acceso a páginas no deseadas. Adicionalmente se podrá evitar la descarga de archivos desde Internet evitando así la posibilidad de ingreso de virus además de bloquear el acceso a sitios de alto consumo de ancho de banda (Videos online, radios, etc.).

Características de Administración: Deberá proveer una interfaz gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interfaz debe soportar SSL sobre HTTP (HTTPS).

Para el servicio, toda actualización no insumirá para la Municipalidad de Luján de Cuyo cargo alguno en concepto de: actualización o cambio de firmware o hardware del equipamiento, durante el plazo contractual de prestación del servicio.

La oferta ganadora fue la perteneciente a la firma Century Link la cual cumplió en su totalidad con los requerimientos del mencionado pliego.

2. INFRAESTRUCTURA DE SERVIDORES

A través de la solicitud 933 del 2019 se inició el procedimiento administrativo para adquirir los siguientes elementos relacionados con la infraestructura de servidores destinados a optimizar el funcionamiento del sistema de gestión y subsistemas informáticos críticos de oficinas y dependencias municipales del Parque Cívico Luján de Cuyo, sito en Calle Mariano Boedo 385 de Luján de Cuyo, Provincia de Mendoza:

- Un (1) chasis del tipo blade con 3 servidores del tipo blade x86, cuyas características se describen en el ítem n°1 del pliego de especificaciones técnicas.
- Una solución de almacenamiento masivo externo de datos (storage), cuyas características se describen en el ítem n°2 del pliego de especificaciones técnicas.
- Dos switches, cables y accesorios para el armado de la red de almacenamiento (san), de acuerdo a lo descripto en el ítem n°3 del pliego de especificaciones
- Una licencia de software de virtualización de servidores, de acuerdo lo descripto el ítem n°4 del pliego de especificaciones técnicas.
- Servicios de instalación, configuración, capacitación y soporte post-instalación conforme se detalla en el ítem n°5 del pliego de especificaciones técnicas.
- Provisión con el conjunto de la solución de 2 notebook de última generación, conforme se detalla en el ítem n°6 del pliego de especificaciones técnicas.

A continuación se describirán algunas de las características que contempla el pliego de especificaciones técnicas:

La tecnología, aplicaciones y servicios ofrecidos deben contribuir a:

- Aumentar a darle versatilidad y flexibilidad a la plataforma soporte de los sistemas que actualmente posee el Municipio y las evoluciones tecnológicas que el mercado ofrezca en el futuro.
- Lograr la más alta calidad y velocidad de respuesta de los sistemas de gestión internamente en el palacio municipal (ejemplo sala de reuniones operativas, salas de coworking y de gabinete, Centro de atención Unificada) y hacia los vecinos.
- Aumentar la velocidad de transferencia y flujo de datos actuales.
- Reducción de los tiempos de espera en el procesamiento para mejorar la experiencia tanto del usuario interno como de los ciudadanos que consultan e interactúan con los sistemas del Municipio y trámites en general.

El adjudicatario deberá proveer cursos de transferencia tecnológica y de capacitación al personal técnico de la Dirección de Informática y Comunicaciones. Dichos cursos tendrán que tener un nivel medio y avanzado, asociados a la Infraestructura y configuración de los recursos de hardware y software a proveerse, diseñar, instalar y configurar en el Parque Cívico Luján de Cuyo.

Garantía: soporte y garantía oficial otorgada por el fabricante por tres (03) años, debiendo estar disponible días y horarios laborales, con un tiempo máximo de respuesta del próximo día laboral (NBD). La garantía de funcionamiento y el servicio técnico de mantenimiento será integral; es decir, que comprenderá el servicio de reparación con provisión de repuestos y/o cambio de las partes que sean necesarias sin cargo alguno para el Municipio. El proveedor garantizará y acreditará por escrito que el servicio técnico será brindado por personal especializado de la empresa fabricante de los productos ofrecidos.

La oferta ganadora fue la de la empresa CEDI CONSULTING S.R.L la cual cumplió con las especificaciones técnicas.

Imagen 10 y 11: Infraestructura Servidores en proceso Parque Cívico

3. SISTEMAS DE GESTIÓN

El sistema de gestión que actualmente posee el Municipio es el sistema MAJOR cuyas características se enuncian a continuación:

- **Sistema de ventana única**

El mismo consiste en que el usuario interno puede definir la totalidad de los atributos que conforman un trámite y su flujo dentro de la organización, estableciendo los controles, estados, secuencias, restricciones, etc., que el mismo posee. Esto es almacenado en una base de datos de definición de trámite.

El usuario externo a la organización brinda los datos que le son requeridos por un motor de definición de trámites, el que explota la base de definiciones mencionada anteriormente.
Esta información puede ser íntegramente digital, incluyendo la captura de imágenes de documentos de identidad, planos, etc.

Una vez incorporado los datos, el motor de proceso se encarga de controlar el flujo de la información dentro de la organización, donde cada área realiza las tareas que le corresponden, habilitando con su conclusión, las siguientes tareas dentro del flujo, hasta la terminación definitiva del trámite.

- **Tablero de Comando**

Permite establecer y controlar indicadores directamente alimentados por el resto de los módulos, o cargados desde otras fuentes, esto permite establecer alarmas y controlar la evolución con datos actualizados en tiempo real.

- **Información Geográfica**

Ofrece la visualización de las Bases de Datos en un mapa digitalizado, permitiendo el análisis de la información a través de la integración de las Bases de Datos con un mapa digitalizado.
A su vez permite optimizar la recaudación, el desarrollo de políticas públicas en cuanto a la salud, seguridad, control ambiental, obras privadas y públicas, control de tránsito, luminarias, etc. Asimismo su exclusiva tecnología de representación permite volcar la información de cualquier capa definida en archivos shp convencionales sobre imágenes satelitales o cartografía.

Algunos de los beneficios del mencionado sistema son los siguientes:

- Centralización y estandarización de trámites.
- Gerenciamiento por proceso.
- Seguridad de la información física al evitar el movimiento de documentos o comprobantes. (digitalización)
- Seguimiento de estado de gestión.
- Control de Gestión.
- Integración de los sectores de la organización.

Los módulos que integran el sistema son: Ingresos Públicos, Contabilidad, Contrataciones, Tesorería, Bienes Físicos, Almacenes, Presupuesto, Crédito Publico, Inversión Pública, Recursos Humanos, Mesa de Entrada, Tribunal de Faltas e Inspección, Contac Center, Gestión de Cobranzas, Cobro por vía de Apremio, Salud, Información Geográfica (GIS), Información de Gestión, Tablero de Control, Ventanilla Única y un sistema Web que comprende la consulta, emisión y pago de tasas y deudas, presentación de DDJJ y consulta de Expedientes.

Además del sistema MAJOR, el Municipio posee diversos sistemas WEB desarrollados internamente que no se encuentran integrados al mismo, aproximadamente hay 40 sistemas, entre ellos se puede mencionar el sistema MLC para control de combustible, el sistema de control de depósitos, el de horarios del personal, etc.

La empresa que proporciona el servicio es COMPUBECCAR S.A con la cual se mantiene el contacto continuo para solucionar cualquier inconveniente o error del sistema, existe un agente municipal encargado de esta tarea el cual también se encarga de brindar capacitaciones continuas ante nuevos módulos o actualizaciones de los existentes. Suelen ayudar en esta tarea otros dos agentes que se desempeñan en el área de informática y comunicaciones.

La municipalidad actualmente no cuenta con procedimientos estandarizados para el mantenimiento de dicho sistema como por ejemplo para controlar las versiones o gestionar el cambio.

En resumen en el presente capítulo se abordaron conceptos referidos a las redes informáticas y sistemas de gestión con los principales problemas de seguridad relacionados con los mismos, aplicando tales contenidos al Municipio bajo análisis en donde se añade como medida de seguridad importante la infraestructura de los servidores adoptada en el Parque Cívico Municipal ubicado en calle Boedo de Carrodilla.

CAPÍTULO VI:
ACCIONES PREVENTIVAS: MEDIDAS DE PROTECCIÓN, POLÍTICAS DE SEGURIDAD Y PLAN DE CONTINGENCIAS

En este capítulo se desarrollarán las acciones preventivas a tener en cuenta para los factores de riesgo y amenazas descriptas en los capítulos anteriores, tales acciones se materializan en medidas de protección, políticas de seguridad y elaboración de un adecuado plan de contingencias. Al igual que en los mencionados capítulos se culmina con la aplicación de estos conceptos a la institución objeto de estudio.

A.PROTECCIÓN

Una vez conocidas las vulnerabilidades y ataques a las que está expuesto un sistema es necesario conocer los recursos disponibles para protegerlo.

Por regla general, las políticas son el primer paso que dispone a una organización para entrar en un ambiente de seguridad, puesto que reflejan su "voluntad de hacer algo" que permita detener un posible ataque antes de que éste suceda. A continuación se citan algunos de los sistemas y sus métodos de protección más comúnmente empleados:

1. SISTEMAS DE DETECCIÓN DE INTRUSOS:

Son sistemas que permiten analizar las bitácoras de los sistemas en busca de patrones de comportamiento o eventos que puedan considerarse sospechosos, sobre la base de la información con la que han sido previamente alimentados. Pueden considerarse como monitores.

a.Trampas de Red

Son sistemas que se activan con la finalidad específica de que los expertos en seguridad puedan observar en secreto la actividad de los Hackers/Crackers en su hábitat natural. Consiste en activar un servidor y llenarlo de archivos tentadores, hacer que sea difícil, pero no imposible penetrarlo y sentarse a esperar que aparezcan los intrusos.

2. SISTEMAS ORIENTADOS A CONEXIÓN DE RED:

Monitorizan las conexiones que se intentan establecer en una red o equipo en particular, siendo capaces de efectuar una acción sobre la base de métricas como: origen y destino de la conexión, servicio solicitado, permisos, etc. Las acciones que pueden emprender suelen ir desde el rechazo de la conexión hasta alerta al administrador. En esta categoría están los cortafuegos (Firewalls) y los Wrappers.

a.Firewall

Es un sistema (o conjunto de ellos) ubicado entre dos redes y que ejerce una política de seguridad establecida. Es el mecanismo encargado de proteger una red confiable de una que no lo es (por ejemplo Internet).

b.Wrappers

Un Wrapper es un programa que controla el acceso a un segundo programa, cubriendo la identidad de este segundo programa y obteniendo con esto un más alto nivel de seguridad. Estos programas nacieron por la necesidad de modificar el comportamiento del sistema operativo sin tener que modificar su funcionamiento. Consiste en un programa que es ejecutado cuando llega una petición a un puerto específico. Este, una vez comprobada la dirección de origen de la petición, la verifica contra las reglas almacenadas, y en función de ellas, decide o no dar paso al servicio.

Adicionalmente, registra estas actividades del sistema, su petición y su resolución.

3. SISTEMAS DE ANÁLISIS DE VULNERABILIDADES:

Analizan sistemas en busca de vulnerabilidades conocidas anticipadamente. La "desventaja" de estos sistemas es que pueden ser utilizados tanto por personas autorizadas como por personas que buscan acceso no autorizado al sistema.

a.Prueba de Vulnerabilidad

Consiste en un modelo que reproduce intentos de acceso, a cualquier entorno informático, de un intruso potencial desde los diferentes puntos de entrada que existan, tanto internos como remotos.

4. SISTEMAS DE PROTECCIÓN A LA INTEGRIDAD DE INFORMACIÓN:

Sistemas que mediante criptografía o sumas de verificación tratan de asegurar que no ha habido alteraciones indeseadas en la información que se intenta proteger.

a.Sistema de detección de intrusos (IDS)

Un sistema de detección de intrusos (IDS) es un proceso o dispositivo activo que analiza la actividad del sistema y de la red por entradas no autorizadas y/o actividades maliciosas. La forma en que un IDS detecta las anomalías pueden variar ampliamente; sin embargo, el objetivo final de cualquier IDS es el de atrapar a los perpetradores en el acto antes de que hagan algún daño a sus recursos. Este tipo de sistema también es válido para proteger la privacidad de la información.

5. SISTEMAS DE PROTECCIÓN A LA PRIVACIDAD DE LA INFORMACIÓN:

Herramientas que utilizan criptografía para asegurar que la información sólo sea visible para quien tiene autorización. Su aplicación se realiza principalmente en las comunicaciones entre dos

entidades.

a. Gestión de claves seguras

Se debe mantener una política de cambio de contraseñas de manera periódica, en la que utilice contraseñas más fuertes para proteger sus datos. Se recomienda que exista diversidad en la construcción de los passwords mediante el uso caracteres alfanuméricos, caracteres especiales y en combinación, con una longitud mínima de 8 caracteres y que se pueda recordar fácilmente, debido a que las contraseñas más largas son mejores al necesitar más tiempo por parte de los agresores para descifrarlas y burlar esa protección. No usar nombres de seres queridos (incluidas mascotas) como contraseñas debido a que existe evidencia que demuestran que las personas no tienen conciencia de compartir esta información con los compañeros del trabajo, exponiéndolas con notas adhesivas en los monitores inclusive, y usando ese criterio como primera opción en un cambio de clave. Aunque las contraseñas fuertes ofrecen una buena protección contra los incidentes de seguridad, estas no dejan de ser infranqueables para aquellos que pretenden acceder a su información y que pueden estar muy cerca de lo que se imagina.

6. ANTIVIRUS

Un antivirus es una gran base de datos con la huella digital de todos los virus conocidos para identificarlos y también con las pautas que más contienen los virus. Los fabricantes de antivirus avanzan tecnológicamente casi en la misma medida que lo hacen los creadores de virus. Esto sirve para combatirlos, aunque no para prevenir la creación e infección de otros nuevos.

Actualmente existen técnicas, conocidas como heurísticas, que brindan una forma de "adelantarse" a los nuevos virus. Con esta técnica el antivirus es capaz de analizar archivos y documentos y detectar actividades sospechosas. Esta posibilidad puede ser explotada gracias a que de los 6–20 nuevos virus diarios, sólo aparecen unos cinco totalmente novedosos al año.

Debe tenerse en cuenta que:

- Un programa antivirus forma parte del sistema y por lo tanto funcionará correctamente si es adecuado y está bien configurado.
- No será eficaz el 100% de los casos, no existe la protección total y definitiva.

Las funciones presentes en un antivirus son:

- Detección: se debe poder afirmar la presencia y/o accionar de un VI en una computadora. Adicionalmente puede brindar módulos de identificación, erradicación del virus o eliminación de la entidad infectada.
- Identificación de un virus: existen diversas técnicas para realizar esta acción (scaning, heurística y chequeadores de integridad)

Es importante diferencia los términos detectar: determinación de la presencia de un virus e identificar: determinación de qué virus fue el detectado. Lo importante es la detección del virus y luego, si es posible, su identificación y erradicación.

B.POLÍTICAS DE SEGURIDAD

La RFC 1244 define Política de Seguridad como: "una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requerirán"

Es indispensable en toda organización que posea activos informáticos contar con políticas de seguridad documentadas y procedimientos internos de la organización acerca de las estrategias y disposiciones que guíen los principales rubros y áreas relacionados con la seguridad de los bienes informáticos y que permitan su actualización y revisión por parte de un comité de seguridad interno.

Algunos de los principales objetivos de control y acciones dentro de este dominio son:

- Políticas de acceso a instalaciones sensibles.
- Políticas y procedimientos de inventarios de bienes informáticos
- Políticas y procedimientos de respaldo de datos.
- Políticas y procedimientos de resguardo de información.
- Políticas y procedimientos para asignación de usuarios y lineamientos normativos de acceso
- Políticas y procedimientos para la creación y mantenimiento de software.

Si bien las herramientas y las aplicaciones forman la base técnica de la política de seguridad, la política de uso aceptable considera otros aspectos:

- Quién tiene permiso para utilizar los recursos
- Quién está autorizado a conceder acceso y a probar los usos
- Quién tiene la administración del sistema
- Qué se debe hacer con la información confidencial
- Cuáles son los derechos y responsabilidades de todos los usuarios

Por ejemplo, al definir los derechos y responsabilidades de los usuarios, se debe analizar:

- Si los usuarios se encuentran restringidos, y cuáles son estas restricciones.
- Si los usuarios pueden compartir cuentas o dejar que otros usuarios utilicen sus cuentas.
- Cómo debería ser el mantenimiento de las cuentas de los usuarios.
- La frecuencia con la que deben cambiar sus contraseñas.
- Si se facilitan copias de seguridad o son los usuarios los que deben realizar las suyas.

Cualquier política de seguridad ha de contemplar las características de la información mencionadas en el Capítulo I, (Integridad, Disponibilidad, Privacidad, Control y Autenticidad) ya que comprenden una descripción de lo que deseamos proteger y el porqué de ello.

1. EVALUACIÓN DE RIESGOS

Este es el proceso de examinar todos los riesgos y valorarlos por niveles de seguridad. El riesgo se materializa cuando una amenaza actúa sobre una vulnerabilidad y causa un impacto. Los gestores deben implantar aquellas medidas de seguridad que lleven los riesgos hasta niveles aceptables, contando para ello con: el costo de las medidas a implantar, la probabilidad que sucedan cada uno de los problemas posibles, el valor de los bienes a proteger y la cuantificación de las pérdidas que podrían derivarse de la aparición de determinado incidente de seguridad, es decir, obtener una evaluación económica del impacto de estos sucesos.

Una vez obtenida la lista de cada uno de los riesgos se efectuará un resumen del tipo:

Imagen 6: Tipo de Riesgo–Factor

Tipo de riesgo	**Factor**
Robo de hardware	Alto
Robo de información	Alto
Vandalismo	Medio
Fallas en los equipos	Medio
Virus informáticos	Medio
Equivocaciones	Medio
Accesos no autorizados	Medio
Fraude	Bajo
Fuego	Muy Bajo
Terremotos	Muy Bajo

Fuente: Borghello, Cristian Fabián (2001). Seguridad Informática: Sus implicancias e implementación

a.Identificación de Amenazas y su impacto

Una amenaza es cualquier circunstancia con el potencial suficiente para causar pérdida o daño del sistema.

Pueden provenir de personas (hackers, crackers), de programas, de sucesos naturales, etc. Equivalen a los factores que se aprovechan de las debilidades del sistema.

Se suele dividir las amenazas existentes según su ámbito de acción:

- Desastre del entorno (Seguridad Física).
- Amenazas del sistema (Seguridad Lógica).
- Amenazas en la red (Comunicaciones).
- Amenazas de personas (Insiders–Outsiders).

Los impactos son los efectos nocivos contra la información de la organización al materializarse una amenaza informática. Al suceder incidentes contra la seguridad informática pueden devenir en:

- Disrupción en las rutinas y procesos de la organización con posibles consecuencias a su capacidad operativa.
- Pérdida de la credibilidad y reputación de la organización por parte del consejo directivo de la organización, público en general, medios de información, etcétera.
- Costo político y social derivado de la divulgación de incidentes en la seguridad informática.
- Violación por parte de la organización a la normatividad acerca de confidencialidad y privacidad de datos de las personas.
- Multas, sanciones o fincado de responsabilidades por violaciones a normatividad de confidencialidad.
- Pérdida de la privacidad en registros y documentos de personas.
- Pérdida de confianza en las tecnologías de información por parte del personal de la organización y del público en general.
- Incremento sensible y no programado en gastos emergentes de seguridad.
- Costos de reemplazo de equipos, programas, y otros activos informáticos dañados, robados, perdidos o corrompidos en incidentes de seguridad.

b.Evaluación de Costos

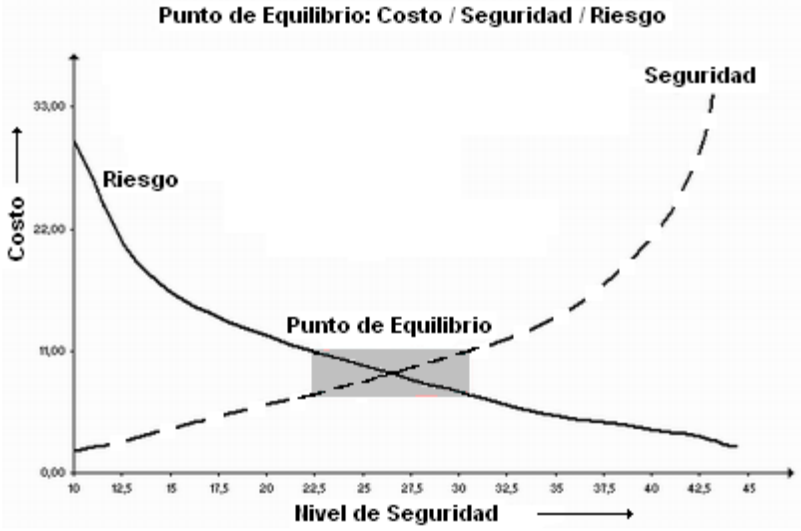
La evaluación de costos más ampliamente aceptada consiste en cuantificar los daños que cada posible vulnerabilidad puede causar teniendo en cuenta las posibilidades. Un planteamiento posible para desarrollar esta política es el análisis de lo siguiente:

- ¿Qué recursos se quieren proteger?
- ¿De qué personas necesita proteger los recursos?
- ¿Qué tan reales son las amenazas?
- ¿Qué tan importante es el recurso?
- ¿Qué medidas se pueden implantar para proteger sus bienes de una manera económica y oportuna?

Con esas sencillas preguntas (más la evaluación de riesgo) se debería conocer cuáles recursos

vale la pena (y justifican su costo) proteger, y entender que algunos son más importantes que otros. El objetivo que se persigue es lograr que un ataque a los bienes sea más costoso que su valor, invirtiendo menos de lo que vale.

Imagen 12: Punto de equilibrio Costo/Seguridad



Fuente: Borghello, Cristian Fabián (2001). Seguridad Informática: Sus implicancias e implementación

Como puede apreciarse los riesgos disminuyen al aumentar la seguridad (y los costos en los que incurre) pero como ya se sabe los costos tenderán al infinito sin lograr el 100% de seguridad y por supuesto nunca se logrará no correr algún tipo de riesgo. Lo importante es lograr conocer cuan seguro se estará conociendo los costos y los riesgos que se corren (Punto de Equilibrio).

C.PLAN DE CONTINGENCIAS: CONCEPTOS, OBJETIVOS Y TIPOS

1. CONCEPTO

Un plan de contingencias es un plan de continuidad que permite a la organización restaurar las operaciones una vez que se ha materializado un desastre de la manera más rápida, eficiente y con el menor costo y pérdidas posibles.

Se entiende como un grupo de medidas preventivas, integradas y coordinadas en una norma única.

2. OBJETIVOS

Cabe aclarar que el objetivo de toda empresa es identificar los tipos de contingencias que puedan afectarla para minimizar el impacto en su operación y agilizar su puesta en funcionamiento en el menor

tiempo posible, por lo tanto lo que pretende este tipo de plan es:

- Definir las actividades de planeamiento, preparación y ejecución de tareas destinadas a proteger la Información contra los daños y perjuicios producidos por corte de servicios, fenómenos naturales o humanos.
- Garantizar la continuidad de las operaciones de los principales elementos que componen los Sistemas de Información.
- Establecer actividades que permitan evaluar los resultados y retroalimentación del plan general

3. TIPOS DE PLANES

a. Plan de respaldo

Contempla las contramedidas preventivas para evitar que se materialice la amenaza.

b. Plan de emergencia

Contempla las contramedidas necesarias para disminuir el efecto de la amenazada materializada.

c. Plan de recuperación

Contempla las medidas necesarias para, una vez materializada y controlada la amenaza, se restauren las cosas al momento previo a la materialización de la amenaza

Para entender mejor lo anteriormente expuesto se brindará un ejemplo práctico: Considerando que la amenaza identificada sea un incendio, los planes a implementar serían los siguientes:

- Plan de respaldo:
  - ❖ Revisión de extintores.
  - ❖ Simulacros de incendio.
  - ❖ Realización de copias de respaldo.
  - ❖ Custodia de las copias de respaldo (por ejemplo, en la caja fuerte de un banco).
  - ❖ Revisión de las copias de respaldo.
- Plan de emergencia:
  - ❖ Activación del precontrato de alquiler de equipos informáticos.
  - ❖ Restauración de las copias de respaldo.
  - ❖ Reanudación de la actividad.
- Plan de recuperación:
  - ❖ Evaluación de daños.
  - ❖ Traslado de datos desde la ubicación de emergencia a la habitual.
  - ❖ Reanudación de la actividad.

- ❖Desactivación del precontrato de alquiler.
- ❖Reclamaciones a la compañía de seguros.

En conclusión el plan de contingencia debe obedecer a un proceso formal y debe ser la conclusión de un proyecto de elaboración del mismo que incluya la identificación de los factores críticos, el establecimiento de los equipos de trabajo y alternativas de solución de la contingencia, una prueba real del mismo plan, una capacitación de las personas involucradas y una constante actualización.

D.MUNICIPALIDAD DE LUJÁN DE CUYO

1. MEDIDAS DE PROTECCIÓN

El Municipio posee antivirus gratuitos en todas las máquinas de trabajo y antivirus de mayor calidad (pagos) en algunas PC. Con respecto al inventario de bienes informáticos sí posee un procedimiento para su relevamiento y posterior registro a través del área de Patrimonio Municipal la cual se encuentra en el sector de Contabilidad Central. Los bienes susceptibles de ser inventariados son aquellos que superan un valor de $1000 aproximadamente. El área de informática posee un registro propio para elementos que no superen este valor. Con respecto al respaldo de datos hay 2 sistemas que cumplen esta función: una es de servidor a servidor y el otro es de réplica de un almacenador. Uno se encuentra en el edificio de Hacienda y el otro en donde se encuentra el Concejo Deliberante (Edificio Taboada).

2. POLÍTICAS DE SEGURIDAD

Actualmente no se poseen políticas de seguridad para adquirir, instalar o supervisar los elementos recomendados universalmente para la seguridad física. De acuerdo a lo expresado, anteriormente sí certificaban normas ISO pero ante la expansión de la organización y la falta de infraestructura esta situación no continuó dentro de sus posibilidades.

En cuanto a las políticas de la seguridad lógica como se mencionó en capítulos anteriores hay un encargado de asignar los usuarios y disponer los lineamientos normativos de acceso en el cual se establece el tratamiento de la información confidencial y cuáles son los derechos y responsabilidades de todos los usuarios. Sin embargo no hay un procedimiento escrito con respecto a si los usuarios pueden compartir cuentas o dejar que otros usuarios utilicen sus cuentas ni del mantenimiento de las mismas. Tampoco se visualiza un procedimiento que establezca la frecuencia con la cual deben cambiar sus contraseñas.

En cuanto a las copias de seguridad las mismas se realizan con respecto a los datos contenidos en el sistema MAJOR, la persona encargada de esta tarea lo efectúa a través de un sistema automático

de backups. Para la información almacenada en cada PC de trabajo no hay un procedimiento establecido y son los propios agentes los que se deben encargar de esta tarea.

3. PLAN DE CONTINGENCIAS

Actualmente se cuenta con un plan de contingencias el cual incluye la identificación de los factores críticos, el establecimiento de los equipos de trabajo y alternativas de solución de la contingencia, una prueba real del mismo plan y una capacitación de las personas involucradas. Ante el caso de que la amenaza identificada sea un incendio de un servidor, el plan de respaldo es que el Municipio posee extintores especiales, el plan de emergencia es que existen 2 réplicas y también un sistema automático de backups y el plan de recuperación sería instalar de nuevo otro servidor. Esta última solución también se adoptó para un caso ocurrido en donde se aterrizaron los cabezales de un disco.

Recapitulando lo expuesto precedentemente las medidas de protección a aplicar tienen diversos sistemas a través de los cuales se pueden implementar, por otra parte para la aplicación de las políticas de seguridad se debe tener en cuenta la evaluación de riesgos, al cual para disminuirlo hasta niveles aceptables deben tenerse en cuenta una serie de aspectos y situaciones. Otra acción preventiva expuesta es el plan de contingencias el cual posee a su vez distintos tipos de planes los cuales resultan muy necesarios para restaurar las operaciones una vez que se ha materializado el desastre.

CAPÍTULO VII: CONCLUSIONES GENERALES

En cuanto a la Seguridad Física se puede concluir que se poseen medidas de seguridad contra incendios (cortafuegos), picos de tensión (tomas de tierra), energía ininterrumpida (grupos electrógenos y UPS) y conservación general del área de informática (ductos y climatización de los servidores adecuados), sin embargo la seguridad en los accesos de los actuales Edificios del Municipio es limitada ya que si bien, existen guardias de seguridad en los accesos principales no hay un control que identifique las personas que ingresan u otros datos relevantes de las mismas. Con respecto a la oficina de informática la misma posee mayores medidas (cerrojo eléctrico y video vigilancia) que si bien, no aseguran una total protección es un avance sustancial en función a las condiciones de esta oficina años atrás. Con respecto a la seguridad de los accesos del parque cívico (Edificio al que se trasladará la mayor parte de la Municipalidad) se detecta la gran evolución acaecida en esta materia, contemplada a través de las especificaciones técnicas requeridas para esta contratación, las cuales se consideran completas y muy efectivas para lograr un alto nivel de seguridad. Por lo anteriormente expuesto se sugiere evaluar y controlar permanentemente la seguridad física del edificio en aspectos en los que no se han adoptado las suficientes medidas, como terremotos e inundaciones ya que será la base para comenzar a integrar la seguridad como una función primordial dentro del Municipio.

En cuanto a los controles de accesos que contribuyen a la seguridad lógica, si bien existen medidas para el acceso al sistema de gestión principal no se poseen para el acceso a la información contenida en las PCs, ni tampoco procedimientos que controlen este tipo de situaciones generando mayor vulnerabilidad a diversos ataques por parte, principalmente, de los mismos empleados. Con respecto a la administración de la seguridad se detecta que no existe un manual de procedimientos escrito en la organización con respecto a aspectos relacionados con la seguridad informática pero sí una auditoría de la base de datos y un registro de memorias de usos y accesos a la misma, por lo que se puede concluir que el nivel de seguridad lógica se encuentre con algunos aspectos para analizar y sobre los cuales invertir recursos y esfuerzos para evitar los riesgos asociados a los mismos.

Con respecto a los delitos informáticos sufridos, los mismos se debieron a la falta de medidas de protección adecuadas relacionadas con este tema. En referencia al inventario de los bienes informáticos se detecta que se lleva un registro por parte del área de informática de los insumos inferiores a $1000 y no en el sistema MAJOR debido a que los mismos no impactan contablemente en el patrimonio municipal, sin embargo su incorporación en el sistema de gestión Municipal a través del módulo de Almacenes se encuentra en proceso con el fin de controlar de manera adecuada y eficiente estos activos. En relación al sistema de respaldo se considera que el mismo cumple con los estándares de seguridad mínimos debido a que se cuenta con un sistema automático de backups para la información

almacenada en el sistema de gestión pero no para la información propia que se posee en el equipamiento de cada agente municipal por lo que deberían aunarse esfuerzos para mejorar este punto. Se sugiere la realización de un análisis de costo/beneficio acerca de la implementación de políticas de seguridad como por ejemplo volver a la certificación de normas ISO. Estas políticas proporcionan las bases para definir y delimitar responsabilidades con el fin de determinar las estrategias y disposiciones que guían los principales aspectos de seguridad a tener en cuenta. En materia de comunicaciones y sistemas se pudo observar que el uso de internet se encuentra controlado y medido, y que el servicio cuenta con muchas características que hacen que la navegación se realice en forma rápida y segura. El sistema de gestión tiene amplias herramientas para realizar auditorías informáticas y otros controles de seguridad, dichas herramientas son explotadas en la actualidad por el área de auditoría y control de gestión por lo que se considera que tanto el sistema de gestión como la administración de la seguridad son buenos, sin embargo en un futuro debería tratarse de integrar los sistemas WEB desarrollados internamente al sistema MAJOR debido a que los mismos poseen muchas falencias de seguridad y faltas de controles.

Como conclusión general se puede decir que debe continuarse en este esfuerzo permanentemente para mantener al día la metodología, las políticas de seguridad, los procedimientos, los controles y las medidas de seguridad de los activos informáticos manteniendo siempre así un nivel de seguridad adecuado y una administración del riesgo razonable; todo ello a un costo proporcional y razonable al valor de los bienes informáticos guardados por lo que se sugiere revisar periódicamente mediante un plan al efecto las normas, políticas, procedimientos y controles de la seguridad informática para perfeccionarlos y mantenerlos actualizados, migrar periódicamente hacia las nuevas versiones de los estándares metodológicos (esto significaría migrar hacia la certificación de las ISO / IEC 27002 y sus derivados, por ejemplo), obtener siempre mediciones acerca de los inventarios, auditorías, bitácoras, etcétera para lograr algunas estrategias y controles que siempre faltan por implementar en el Municipio o que deben perfeccionarse debiendo hacerse una revisión equivalente para evaluar los riesgos y actuar al efecto.

BIBLIOGRAFÍA

- Ley 11723 Propiedad Intelectual**.** Boletín Oficial, Buenos Aires, 30 de Septiembre de 1933.
- Ley 25326 Protección de los datos personales. Boletín Oficial, Buenos Aires, 2 de Noviembre de 2000.
- Ley 26388 Modificación Código Penal. Boletín Oficial, Buenos Aires, 25 de Junio de 2008.
- Alvort, D. (2012, 24 de noviembre). *Seguridad Informática*. [en línea]. Recuperado de http://seguridad-infomatica.blogspot.com/2012/11/seguridad-logica.html. [jul/19].
- Apuntes de la cátedra de Auditoría Operativa de la Universidad Nacional de Cuyo.
- Asensio, G. (2006). *Seguridad en Internet: Una guía práctica y eficaz para proteger su PC con software gratuito*. Madrid: Ediciones Nowtilus. Recuperado de http://bookparadise.online/pdf?title=Seguridad+en+Internet%3A+Una+gu%C3%ADa+pr%C3%A1ctica+y+eficaz+para+proteger+su+PC+con&geo=es&i=OTc4LTg0OTc2MzI5MzU%3D&src=google. [jul/19].
- Basaes, J., Godoy, V., Reitano, J., Rojas Gaete, D., Rossel Ortega M.L. y Rossel Ortega, M. (2014). El rol del auditor operativo. Importancia del contador como auditor operativo en el contexto actual. (Trabajo de Investigación Contador Público, Universidad Nacional de Cuyo). Recuperado de http://bdigital.uncu.edu.ar/objetos_digitales/6692/basaesgodoyreitanogaeterosselortega-tesisfce.pdf. [jul/19].
- Borghello, Cristian Fabián (2001). Seguridad Informática: Sus implicancias e implementación. (Tesis de Licenciatura en Sistemas, Universidad Tecnológica Nacional). Recuperado de http://www.segu-info.com.ar/tesis/tesis-borghello-full.zip. [jul/19].
- Candelario Samper, J.J y Rodriguez Bolaño, J. (2015). Seguridad informática en el siglo XX: Una perspectiva jurídica tecnológica enfocada hacia las organizaciones nacionales y mundiales, *Publicaciones e Investigación*, Vol. 9, 153-162. Recuperado de http://portal.bibliotecas.utn.edu.ar/proxy/https://doaj.org/article/980d4dcb20164454bd9b0f88d2828bf3. [jul/19].
- Contraloría Municipal de Villavicencio. (2018, 8 de Mayo). *Plan de Contingencia Informática.* [en línea]. Recuperado de https://contraloriavillavicenciometa.micolombiadigital.gov.co/sites/contraloriavillavicenciometa/content/files/000086/4286_plagt03-plan-de-contingencia-informatica.pdf. [jul/19].
- Chacón, J.F. (s.f). *Sistemas informáticos: Estructuras y funciones. Elementos de hardware. Elementos de software.* [en línea]. Madrid: Preparadores de oposiciones para la enseñanza.

Recuperado de https://www.preparadores.eu/temamuestra/PTecnicos/PComerciales.pdf. [jul/19].

- Descalzo, F. (2016, 25 de Noviembre). *La importancia del factor humano.* [en línea]. México: Revista especializada MAGAZCITUM© CYBSEC. Recuperado de http://www.cybsec.com/upload/Magazcitum_La_importancia_del_factor_%20humano.pdf. [jul/19].
- Eibin, F. & Miguel Ángel, Ch. (2013). Diseño e implementación de un Honeypot para la empresa SOLUCONSTRUCCION SAS. (Proyecto de Grado, Universidad Piloto de Colombia). Recuperado de http://polux.unipiloto.edu.co:8080/00000807.pdf. [jul/19].
- Jaramillo, C. (2017). *2da Disquisición sobre la verdad, la justicia, la libertad y los derechos humanos*. Bloomington: Palibrio. Recuperado de https://play.google.com/books/reader?id=BzFDDwAAQBAJ&hl=es_419&pg=GBS.PT24.w.5.0.42. [jul/19].
- Marin, M.A. y Taboas, D. (2013). Argentina y las TIC: Problemas y Desafíos, *Revista de la Facultad de Ciencias Económicas 2014*, 130. Recuperado de http://bdigital.uncu.edu.ar/6995. [jul/19].
- Ministerio del Interior de España. (2013). *Cibercriminalidad.* [en línea]. Recuperado de http://www.interior.gob.es/documents/10180/1207668/Avance+datos+ciberciminalidad+2013.pdf/5de24ec6-b1cc-4451-bd06-50d93c006815. [jul/19].
- *¿Qué es una contraseña o password? - Definición de contraseña o password*. (s.f). [en línea]. Recuperado de https://www.masadelante.com/faqs/password [jul/19].
- Raffino, M. (2019, 29 de agosto). *"Concepto de redes informáticas"*. [en línea]. Recuperado de https://concepto.de/redes-informaticas/#ixzz60AVZLiNh [ago/19].
- Rendón Burgos, K. y Merizalde Zamora Y.H. (2016). La gestión de la seguridad informática empleando las normas ISO 27001:2013, *Opuntia Brava*, Vol 8. Recuperado de http://portal.bibliotecas.utn.edu.ar/proxy/https://doaj.org/article/5c061efaa43947de8f1cfb9b258ea291. [jul/19].
- Rocha-Haro, C.A. (2011). La seguridad informática, *Ciencia UNEMI*, Vol. 4, 26-33. Recuperado de http://portal.bibliotecas.utn.edu.ar/proxy/https://doaj.org/article/4bf0d3c7763544bbb994728497aa1c50. [jul/19].
- *Tipos de Amenazas Humanas.* [en línea] (2017, 10 de Febrero). Recuperado de https://seguridadeinformaticabrm.wordpress.com/2017/02/10/tipos-de-amenazas-humanas/. [jul/19].

- Voutssas M., J. (2010). Preservación documental digital y seguridad informática, *Investigación bibliotecológica*, 24(50), 127-155. Recuperado de http://portal.bibliotecas.utn.edu.ar/proxy/http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008&lng=en&tlng=en. [jul/19].
- Universidad Internacional de Valencia. *Conceptos sobre seguridad lógica informática.* (2018, 1 de Marzo). Valencia, España: Ciencia y Tecnología. Recuperado de https://www.universidadviu.com/conceptos-seguridad-logica-informatica/. [jul/19].
- USS SEGURIDAD. (2018, 23 de julio). *Tipos de control de acceso de seguridad informática: ¿Cuántos hay y qué características tienen*? [en línea]. Blog de Seguridad para Empresas. Recuperado de https://uss.com.ar/corporativo/tipos-de-control-de-acceso-de-seguridad-informatica/. [jul/19].

UNCUYO UNIVERSIDAD NACIONAL DE CUYO — FACULTAD DE CIENCIAS ECONÓMICAS

DECLARACIÓN JURADA RESOLUCIÓN 212/99 CD

El autor de este trabajo declara que fue elaborado sin utilizar ningún otro material que no haya dado a conocer en las referencias que nunca fue presentado para su evaluación en carreras universitarias y que no transgrede o afecta los derechos de terceros.

Mendoza, 21 de octubre de 2019

Noelia B. Elías

Firma y aclaración

26629

Número de registro

35926 036

DNI

1