**Introducción**

El objetivo de este Protocolo, elaborado por la Secretaria de Tecnologías de la información y las Comunicaciones de la Alcaldía de Armenia, es establecer, como medida de autorregulación, un procedimiento estandarizado para la prevención de incidentes de delito informático.

El presente Protocolo está dirigido para el área de Tesorería Municipal.

**1. Definiciones**

**1.1 Nodo Principal:** Equipo a cargo de la Tesorera Municipal, en el cual se realizaran los pagos.

**1.2 Nodos Secundarios:** Equipos en los cuales se genera el archivo plano para el pago de Contratistas y Nomina.

1.4 Fraude informático (fraude electrónico): Es la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, donde se influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema. (Referencia Código Penal, Ley N° 1273 de 2009).

1.5 Phishing: Fraude tradicionalmente cometido a través de internet, que pretende conseguir datos confidenciales de usuarios, tales como identificación o claves de acceso a cuentas de diversos sistemas. Para lograr este objetivo, generalmente se realizan envíos masivos de correos electrónicos (email), que simulan provenir de entidades de confianza, advirtiéndole a la víctima que, por "motivos de seguridad" o con el fin de "confirmar su cuenta", entre otros, debe suministrar sus datos personales, claves u otra información confidencial, para lo cual se utiliza un sitio web fraudulento y se requiere a la víctima a que haga “click” en un enlace (link) incluido en el mensaje. Posteriormente, con esta información confidencial, los delincuentes realizan transferencias a cuentas de terceros y retiran el dinero.

1.6 Pharming: Modalidad de estafa online (en línea) mediante la manipulación de los servidores DNS (Domine Name Server) para re-direccionar el nombre de un dominio, visitado habitualmente por el usuario, a una página web idéntica a la original, que ha sido creada para obtener datos confidenciales de usuarios como identificación o claves de acceso a cuentas de diversos sistemas.

1.7 OTP:One time password, tecnología que permite generar una clave para uso en una única oportunidad, como por ejemplo token (virtuales o físicos), tarjetas de claves dinámicas, entre otros.

1.8 Phreaking: Hacking orientado a la telefonía y estrechamente vinculado con la electrónica aplicada a los sistemas telefónicos.

1.9 Vishing: Es una variante del phishing, pero por teléfono. Consiste en el envío de un correo electrónico en el cual los delincuentes consiguen detalles de datos bancarios mediante un número telefónico gratuito, en la cual una voz computadorizada de aspecto profesional requiere de las víctimas la confirmación de su cuenta bancaria, solicitándoles el número de cuenta, tarjeta, PIN y otros datos confidenciales.

**2. Criterios de seguridad de la información**

2.1 Confidencialidad: Hace referencia a la protección de información cuya divulgación no está autorizada.

2.2 Integridad: La información debe ser precisa, coherente y completa desde su creación hasta su destrucción.

2.3 Disponibilidad: La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.

**3. Criterios de calidad de la información**

3.1 Efectividad: La información relevante debe ser pertinente y su entrega oportuna, correcta y consistente.

3.2 Eficiencia: El procesamiento y suministro de información debe hacerse utilizando de la mejor manera posible los recursos.

3.3 Confiabilidad: La información debe ser apropiada para la administración de la entidad y el cumplimiento de sus obligaciones.

**4. Seguridad y Calidad**

4.1 En el desarrollo de los criterios de seguridad y calidad, La Secretaria de las Tecnologías de la Información y las Comunicaciones, deberá tener todas las herramientas necesarias desde el punto de vista de hardware y software que permitan prevenir, detectar y corregir situaciones de riesgo que comprometan directamente los diferentes servicios, la información bancaria y la información de los usuarios.

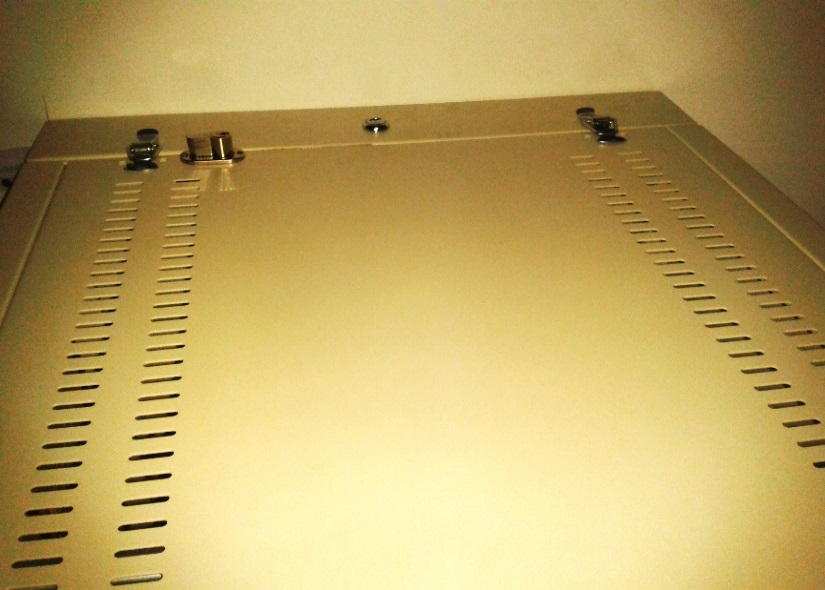
4.2 Como complemento a las herramientas se deberán hacer análisis y retroalimentaciones constantes de frente a las modalidades delictivas su permanente evolución y nuevas formas de materialización, que permitan en consecuencia generar aplicaciones que aumenten, en primera instancia, el nivel de seguridad de los diferentes servicios.

**4.1 El Nodo Principal, posee la siguiente estructura:**

4.1.1 La CPU está protegida físicamente por un Rack (Gabinete Metálico con llave), para evitar cualquier manipulación a nivel de Hacking Hardware y su cableado esta resguardado por una canaleta metálica.

* + 1. El sistema operativo es Windows 7 Professional de 32 bits.
    2. Se deshabilitaron:
       1. Puertos USB
       2. Unidad de CD/DVD
    3. Se asignó dirección IP por DHCP estática.

La dirección IP por motivos de seguridad no se registra en este informe. (Solo el Secretario de Despacho de la Secretaria TIC y el Contratista de Seguridad Informática tienen acceso a dicha información).

* + 1. La IP se encuentra registrada en el portal bancario como IP fija, lo cual no permite realizar transacciones en otro lugar que no corresponda dicha IP.
    2. Cuenta con las políticas de seguridad Active Directory desde el servidor principal.
    3. Para el acceso a los portales bancarios utiliza las restricciones de Páginas de Correo, Redes Sociales, Generación de Historial de navegación, Archivos Temporales y demás elementos ajenos al proceso Web estipulado.
    4. Ningún otro Hardware será reconocido por el sistema si es conectado en el puerto USB donde estará la impresora.
    5. Solo tendrá acceso a internet el personal encargado del manejo de portales bancarios en horario de Lunes a Viernes de 8:00 am a 12:00 pm y de 2:00 pm a 6:00 pm (Los fines de semana y festivos no se proporcionara conexión).
    6. Se realiza Cifrado de los Archivos del sistema, lo cual impedirá que alguien los pueda visualizar al copiarlos fuera de la maquina principal.
    7. Autenticación del usuario antes de que inicie Windows, al encender la maquina se debe ingresar una contraseña para que se inicie el Windows y su posterior Login al dominio con usuario y contraseña respectivos.
    8. La contraseña del Administrador no será de conocimiento de ningún Usuario o Administrador, ya que esta será gestionada por un bunker de contraseñas virtual.
    9. El sistema tiene restringido la instalación o implantación de cualquier programa keylogger, Malware o Virus desde el monitor de aplicaciones del KasperskyEndPoint.



**4.2 Nodos Secundarios.**

Estrategia de Confidencialidad:

* + 1. Por medio del correo institucional se realiza la transferencia de los archivos planos y su posterior pago en la web desde el Nodo Principal.
    2. Para el acceso a los portales bancarios utiliza las restricciones de Páginas de Correo, Redes Sociales, Generación de Historial de navegación, Archivos Temporales y demás elementos ajenos al proceso Web estipulado.
    3. Proteger las claves de acceso a los sistemas de información. En desarrollo de esta obligación, los usuarios deberán evitar el uso de claves compartidas, genéricas o para grupos. La identificación y autenticación en los dispositivos y sistemas de cómputo de la Tesorería Municipal de la Alcaldía de Armenia, deberá ser única y personalizada.
    4. Dotar a sus terminales o equipos de cómputo de los elementos necesarios que eviten la instalación de programas o dispositivos que capturen la información de sus operaciones o su posterior traslados en medios de almacenamiento.

1. **HUMANWARE:** El factor humano que interviene en un sistema. En el campo de los sistemas de información, se refiere generalmente a las personas involucradas y van desde usuarios, desarrolladores de aplicaciones, administradores, operadores Etc.

5.1. **Requisitos del Personal para el Procedimiento de Seguridad Informática en el Nodo Principal, Computador Pagos Tesorería:**

5.1.1 Estar vinculado contractualmente o en cargo administrativo con la Administración Municipal.

5.1.2 Certificar mínimo 48 horas de capacitación en Seguridad Informática con la Administración Municipal o con un ente externo a ella. En caso de ser una entidad externa a la Alcaldía debe presentar las certificaciones en físico.

5.1.3 Ser ingeniero de sistemas, electrónico o áreas a fines.

5.1.4 Firmar compromiso de confidencialidad de Información.

**6. Procedimientos a Realizar**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **6.1 PROCEDIMIENTOS DIARIOS** | | | | |
| **Código** | **Procedimiento** | **Responsable(s)** | **Grupo de Verificación de Procedimiento** | **Formato a Utilizar** |
|  | Verificación Física del Equipo | Profesional Especializado de la Secretaria TIC. | El Contratista de Seguridad Informática de la Secretaria TIC y La Tesorera Municipal |  |
|  | Verificación Lógica del Equipo | Profesional Especializado de la Secretaria TIC. | El Contratista de Seguridad Informática de la Secretaria TIC y La Tesorera Municipal |  |

6.2 Se revisara el equipo de cómputo con el fin de comprobar el la integridad física y lógica del equipo, para dicho procedimiento deben estar presentes el Profesional Especializado de la Secretaria TIC y la Tesorera Municipal. Al final de la revisión se firmara acta de la misma con el formato estipulado y será revisada por el Auditor en Sistemas de gestión de la Seguridad de la Información ISO27001 de la Secretaria TIC.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **6.3 PROCEDIMIENTOS SEMANALES** | | | | |
| **Código** | **Procedimiento** | **Responsable(s)** | **Grupo de Verificación de Procedimiento** | **Formato a Utilizar** |
|  | Cambio de Contraseña Usuario Administrador Equipo | Profesional Especializado de la Secretaria TIC. | El Contratista de Seguridad Informática de la Secretaria TIC y La Tesorera Municipal |  |
|  | Cambio de Contraseña Usuario del Dominio Tesorería Municipal | La Tesorera Municipal | El Contratista de Seguridad Informática de la Secretaria TIC y La Tesorera Municipal |  |

**7. Procedimientos recomendados a llevar a cabo por la Tesorería Municipal.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **7.1 PROCEDIMIENTOS SEMANALES** | | | | |
| **Código** | **Procedimiento** | **Responsable(s)** | **Grupo de Verificación de Procedimiento** | **Formato a Utilizar** |
|  | Cambio de Contraseña Portales Bancarios |  |  |  |
|  | Verificación de Estados Bancarios |  |  |  |

**8. Anexos:**

Adquirir todos los dispositivos y licencias recomendados para la correcta ejecución de las políticas presentes.

**8.1 Licencias:**

8.1.2 Microsoft Windows 7 Professional

8.1.3 KasperskyEnd Point Advance

**9. Recomendaciones**

9.1 Se recomienda por parte de la Secretaria TIC, que anexo a este protocolo de seguridad informática, se realice otro protocolo por la Tesorería Municipal según su criterio, lo anterior para prevenir y detectar posibles anomalías o fraudes electrónicos.

9.2 Se recomienda por parte de la Secretaria TIC, evitar panorámica directa de las cámaras de seguridad de la Administración Municipal, lo anterior para evitar la visualización de contraseñas personales.

Importante: Cuando hablamos de la cualidad de “seguro” o de dimensiones tales como la confidencialidad, no podemos dejar de recordar que son apreciaciones siempre subjetivas y nunca absolutas. Se puede obtener objetivamente un nivel adecuado o razonable de seguridad, de protección de la confidencialidad, pero de ninguna manera podemos hablar de un valor absoluto de la cualidad de seguro. Siempre existen riesgos y debemos contar con ellos.

|  |  |  |
| --- | --- | --- |
| Elaborado por:  **COMITÉ OPERATIVO**  **CALIDAD-MECI** | Revisado por:  **JAIME ALBERTO LLANO CHAPARRO**  Líder del Proceso  Infraestructura Tecnológica | Aprobado por:  **CARLOS FERNANDO BENITEZ ZAPATA**  Gerente de Proceso  Secretaria de Tecnologías de la Información y las Comunicaciones |