SESIÓN EXTRAORDINARIA Nº19-2017

Acta de la Sesión Extraordinaria número diecinueve – dos mil diecisiete, celebrada por la Corporación Municipal de Montes de Oro, el día jueves 09 de febrero del 2017, en el Salón de Sesiones de la Municipalidad de Montes de Oro, al ser las diecisiete horas y doce minutos.

REGIDORES PROPIETARIOS:

Juan Luis León Barrantes - Presidente Municipal

Luis Ángel Trejos Solís –Vicepresidente Municipal

Bernarda Agüero Alpizar

Miguel Ángel Alan Mora

Ana Elizabeth Córdoba Arias

REGIDORES SUPLENTES:

Anthony Fallas Jiménez

Randall Alfaro Peña

José Manuel Alvarado Prendas

SINDICOS PROPIETARIOS:

Roció Vargas Quesada

Lorena Barrantes Porras

SINDICOS SUPLENTES:

Adonay Jiménez Salas

FUNCIONARIOS MUNICIPALES:

Luis Alberto Villalobos Artavia- Alcalde Municipal

Juanita Villalobos Arguedas - Secretaria Municipal

Se somete a consideración el Orden del Día, de la siguiente forma:

ORDEN DEL DÍA:

1-Comprobación del cuórum

2- Audiencias:

2.1. Ing. Gustavo Torres Fernández- Exposición de las Políticas de Seguridad de la Información.

3- Cierre de Sesión

CAPITULO PRIMERO – COMPROBACION DE CUORUM

<u>INCISO Nº1:</u> Comprobado que existe el cuórum, se inicia la Sesión, a las diecisiete horas y doce minutos.
ENTERADOS.

CAPITULO SEGUNDO-AUDENCIA AL ING. GUSTAVO TORRES FERNÁNDEZ- EXPOSICIÓN DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

El Ing. Gustavo Torres Fernández expresa que en una sesión de trabajo con los regidores; ya había expuesto una gran parte de este reglamento y para el día de hoy, va a tratar de terminar de explicar lo que hace falta, que a continuación detalla:

8. GESTIÓNDECOMUNICACIONESYOPERACIONES

Objetivos:

A) Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones.

B) Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y separación de funciones.

Cada Propietario de la Información, junto con el Responsable de Seguridad Informática, determinará los requerimientos para resguardar la información por la cual es responsable. Asimismo, aprobará los servicios de mensajería autorizados para transportar la información cuando sea requerido, de acuerdo a su nivel de criticidad.

8.1. Procedimientos y Responsabilidades Operativas

8.1.1. Documentación de los Procedimientos Operativos

Se documentarán y mantendrán actualizados los procedimientos operativos identificados en esta Política y sus cambios serán autorizados por el Responsable de Seguridad Informática.

8.1.2. Control de Cambios en las Operaciones

Se definirán procedimientos para el control de los cambios en el ambiente operativo y de comunicaciones. Todo cambio deberá ser evaluado previamente en aspectos técnicos y de seguridad.

El Responsable de Seguridad Informática contralora que los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan. El Responsable del Área Informática evaluará el posible impacto operativo de los cambios previstos y verificará su correcta implementación.

8.1.3. Procedimientos de Manejo de Incidentes

Se establecerán funciones y procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad.

8.1.4. Separación de Funciones

Se contemplará la separación de la gestión o ejecución de tareas o áreas de responsabilidad, en la medida de que la misma reduzca el riesgo de modificaciones no autorizadas o mal uso de la información o los servicios por falta de independencia en la ejecución de funciones críticas.

En los casos en los que este método de control no se pudiera cumplir, se implementarán controles tales como el monitoreo de las actividades y/o la elaboración de registros de auditoría y control periódico de los mismos.

8.1.5. Separación entre Instalaciones de Desarrollo e Instalaciones Operativas

Los ambientes de desarrollo, prueba y operaciones, siempre que sea posible, estarán separados preferentemente en forma física, y se definirán y documentarán las reglas para la transferencia de software desde el estado de desarrollo hacia el estado operativo.

8.1.6. Gestión de Instalaciones Externas

En el caso de tercerizar la administración de las instalaciones de procesamiento, se acordarán controles con el proveedor del servicio que se incluirán en el contrato detercerización.

8.2. Planificación y Aprobación de Sistemas

8.2.1. Planificación de la Capacidad

El Responsable del Área Informática, o el personal que éste designe, efectuará el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuados.

Para ello tomará en cuenta además los nuevos requerimientos de los sistemas así como las tendencias actuales y proyectadas en el

procesamiento de la información de la Municipalidad para el período estipulado de vida útil de cada componente. Asimismo, informará las necesidades detectadas a las autoridades competentes para que puedan identifica y evitar potenciales cuellos de botella, que podrían plantear una amenaza a la seguridad o a la continuidad del procesamiento, y puedan planificar una adecuada acción correctiva.

8.2.2. Aprobación del Sistema

El Responsable del Área Informática y/o el Responsable de Seguridad Informática sugerirán criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, solicitando la realización de las pruebas necesarias antes de su aprobación definitiva.

8.3. Protección Contra Software Malicioso

8.3.1. Controles Contra Software Malicioso

El Responsable de Seguridad Informática definirá controles de detección y prevención para la protección contra software malicioso. El Responsable del Área Informática, o el personal designado por éste, implementarán dichos controles.

El Responsable de Seguridad Informática desarrollará procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.

8.4. Mantenimiento

8.4.1. Resguardo de la información

El Responsable del Área Informática y la comisión de Seguridad Informática, determinarán los requerimientos para resguardar cada software o dato en función de su criticidad. En base a ello, se definirá y documentará un esquema de resguardo de la información.

8.4.2. Registro de Actividades del Personal Operativo

El Responsable del Área Informática asegurará el registro de las actividades realizadas en los sistemas, incluyendo según corresponda:

A)Tiempos de inicio y cierre del sistema.

B) Errores del sistema y medidas correctivas tomadas.

C)Intentos de acceso a sistemas, recursos o información crítica o acciones restringidas

D) Ejecución de operaciones críticas

E)Cambios a información crítica

8.4.3. Registro de Fallas

El Responsable del Área Informática desarrollará y verificará el cumplimiento de procedimientos para comunicarlas fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.

8.5. Administración de la Red

8.5.1. Controles de Redes

El Responsable de Seguridad Informática definirá controles para garantizar la seguridad de los datos y los servicios conectados en las redes de la Institución, contra el acceso no autorizado y procederá con su respectiva implementación.

8.6. Administración y Seguridad de los Medios de Almacenamiento

8.6.1. Administración de Medios Informáticos Removibles

El Responsable de Seguridad Informática, implementará procedimientos para la administración de medios informáticos removibles ,como cintas,discos, casetes e informes impresos.

8.6.2. Eliminación de Medios de Información

El Responsable de Seguridad Informática definirá procedimientos para la eliminación segura de los medios de información respetando la normativa vigente.

8.6.3. Procedimientos de Manejo de la Información

Se definirán procedimientos para el manejo y almacenamiento de la información de acuerdo a lo establecido en el capítulo 5 “Clasificación y Control de Activos”.

8.6.4. Seguridad de la Documentación del Sistema

La documentación del sistema puede contener información sensible, por lo que se considerarán los recaudos para su protección, de almacenarla documentación del sistema en forma segura y restringir el acceso a la documentación del sistema al personal estrictamente necesario. Dicho acceso será autorizado por el Propietario de la Información relativa al sistema.

8.7. Intercambios de Información y Software

8.7.1. Acuerdos de Intercambio de Información y Software

Cuando se realicen acuerdos entre organizaciones para el intercambio de información y software, se especificarán el grado de sensibilidad de la información de la Municipalidad y las consideraciones de seguridad sobre la misma.

8.7.2. Seguridad de los Medios en Tránsito

Los procedimientos de transporte de medios informáticos entre diferentes puntos (envíos postales y mensajería) deberán contemplar la utilización de medios de transporte o servicios de mensajería confiable, suficiente embalaje para el envío y la adopción de controles especiales(cuando resulte necesario) a fin de proteger la información sensible contra divulgación o modificación no autorizadas.

8.7.3. Seguridad del Gobierno Electrónico

El Responsable de Seguridad Informática verificará que los procedimientos de aprobación de Software del punto "Aprobación del Sistema" incluyan, para las aplicaciones de Gobierno Electrónico, los siguientes aspectos:

A) Autenticación: Nivel de confianza recíproca suficiente sobre la identidad del usuario y la Municipalidad.

B) Niveles de Autorización adecuados para establecer disposiciones, emitir o firmar documentos clave, etc. Forma de comunicarlo al otro participante de la transacción electrónica.

C) Procesos de oferta y contratación pública: Requerimientos de confidencialidad, integridad y prueba de envío y recepción de documentos clave y de no repudio de contratos.

D)Trámites en línea: Confidencialidad, integridad y no repudio de los datos suministrados con respecto a trámites y presentaciones ante el estado y confirmación de recepción.

E) Verificación: Grado de verificación apropiado para constatar la información suministrada por los usuarios.

F) Cierre de la transacción: Forma de interacción más adecuada para evitar fraudes.

G) Protección a la duplicación: Asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario.

H) No repudio: Manera de evitar que una entidad que haya enviado o recibido información alegue que no la envió o recibió.

I)Responsabilidad: Asignación de responsabilidades ante el riesgo de eventuales presentaciones, tramitaciones o transacciones fraudulentas.

8.7.4. Seguridad del Correo Electrónico

8.7.4.1. Riesgos de Seguridad

Se implementarán controles para reducir los riesgos de incidentes de seguridad en el correo electrónico, contemplando:

A) La vulnerabilidad de los mensajes al acceso o modificación no autorizados o a la negación de servicio.

B) La posible intercepción y el consecuente acceso a los mensajes en los medios de transferencia que intervienen en la distribución de los mismos.

C) Las posibles vulnerabilidades a errores, por ejemplo, consignación incorrecta de la dirección o dirección errónea, y la confiabilidad y disponibilidad general del servicio.

D) La posible recepción de código malicioso en un mensaje de correo, el cual afecte la seguridad de la terminal receptora o de la red a la que se encuentra conectada.

E)El impacto de un cambio en el medio de comunicación en los procesos de la Institución.

F) Las consideraciones legales, como la necesidad potencial de contar con prueba de origen, envío, entrega y aceptación.

G) Las implicaciones de la publicación externa de listados de personal, accesibles al público.

H) El acceso de usuarios remotos a las cuentas de correo electrónico.

I)El uso inadecuado por parte del personal.

8.7.4.2. Política de Correo Electrónico

El Responsable de Seguridad Informática y/o el Responsable del Área Informática definirán y documentarán normas y procedimientos claros con respecto al uso del correo electrónico, que incluya al menos los siguientes aspectos:

A) Protección contra ataques al correo electrónico, por ejemplo virus, intercepción, etc.

B) Protección de archivos adjuntos de correo electrónico.

C) Uso de técnicas criptográficas para proteger la confidencialidad e integridad de los mensajes electrónicos (Ver 10.3. Controles Criptográficos).

D) Retención de mensajes que, si se almacenaran, pudieran ser usados en caso de litigio.

E) Controles adicionales para examinar mensajes electrónicos que no pueden ser autenticados.

F) Aspectos operativos para garantizar el correcto funcionamiento del servicio (ej.: tamaño máximo de información transmitida y recibida, cantidad de destinatarios, tamaño máximo del buzón del usuario,etc.).

G) Definición de los alcances del uso del correo electrónico por parte del Personal de la Municipalidad.

La Regidora Bernarda Agüero Alpizar le pregunta a Gustavo que cuando él no está y pasa algo en informática que se hace?
El Ing. Gustavo Torres responde que la funcionaria Yarline, le colabora cuando él no está; ya que ella tiene conocimiento en informática.
Además, este reglamento es para políticas de seguridad y no es un manual de puestos. Existen políticas de seguridad y de incidentes, en esto estamos hablando de datos. Una cosa es información y otra cosa es información digital.
Además; un auditor puede revisar, pero no puede modificar, ya que su función es fiscalizar.
El Regidor Suplente Anthony Fallas Jiménez expresa que éste es el precio de que éste departamento de informática sea unipersonal, donde todo lo tiene que hacer la misma persona.
El Ing. Gustavo Torres expresa que se debe de implementar en el sistema lo de las denuncias, donde se obtenga datos como: quien la interpuso y el proceso que se llevo a cabo, ya que no hay un seguimiento de las mismas.
El Regidor Luis Ángel Trejos Solís le solicita al Gustavo que le aclare, el caso de las compras, que si se lleva el control del departamento que lo solicita.
El Ing. Gustavo Torres responde que existe un procedimiento: comenzando con una decisión inicial, el cual lleva su consecutivo, el código de la descripción y las firmas respectivas y de ahí arranca el procedimiento; además de las salidas de bodegas de cada funcionario, con su debida descripción.
También; cual es el valor de cada modelo, son varios, todo esto en conjunto con varios departamentos: tesorería, contabilidad, proveeduría y otros departamentos involucrados, no se está

trabajando con una licencia, porque fue diseñado por el departamento de informática.
Los listados de movimientos, es seguridad de la información de datos, la cual tiene que ser veraz y poder resolver cualquier resolución.
El Alcalde Municipal pregunta ¿Quién fiscaliza al Informático?
El Ing. Gustavo Torres responde, que va a existir una comisión de seguridad de la información, la cual velara que las cosas se estén haciendo de la mejor manera.
La Regidora Bernarda Agüero Alpizar pregunta ¿Quiénes va a integrar esta comisión?
El Ing. Gustavo Torres responde que podría ser los encargados de los departamentos, que tengan que ver con los sistemas.
El Alcalde Municipal expresa que no es posible que su persona no tenga acceso a las claves.
El Ing. Gustavo Torres expresa que le puede dar acceso al Alcalde; si se lo solicita por escrito, ya quedaría registrado como un usuario, donde puede verificar los datos. Y que existen roles, que si pasa algo recae sobre su persona.
El Alcalde Municipal Luis Alberto Villalobos Artavia expresa que debe de haber un convenio de confidencialidad.
El Ing. Gustavo Torres expresa que por eso están las políticas, para que haya responsabilidades.
Además, el Alcalde le puede solicitar un informe diario, ya que por encima de cualquier comisión, está el Alcalde.
El Presidente Municipal Juan Luis León Barrantes pregunta ¿que quien vigilaría a esa comisión? si hubiera alguna anomalía.
El Ing. Gustavo Torres responde que para eso está el Auditor (a); ya que si éste Departamento; necesita algo su obligación es darle la información.
El Regidor Suplente Anthony Fallas Jiménez expresa que para eso se va a nombrar una comisión, para fiscalizar y la Administración siempre va a tener el poder generalísimo sobre todo, representado por el Alcalde, el cual va a tener el poder, como máximo jerarca.
El Alcalde Municipal expresa que para que el Informático sea supervisado se debería de contratar un informático externo.
El Ing. Gustavo Torres expresa que si lo contratan; que sea a derecho con su debido contrato.

La Regidora Bernarda Agüero Alpizar pregunta ¿que cuando la funcionaria Yarline hace algo en ese departamento de Informática y si pasara algo, entonces ella es la responsable?.

El Ing. Gustavo expresa que él es el encargado de este departamento y es el responsable de lo que pasa y con estas políticas de seguridad se va a llevar control; tal es el caso que si existiera alguna alteración se detecta quien la realizo. Pero su departamento, no puede modificar nada de otros departamentos. Además, de proteger los datos de la Municipalidad.

El Regidor Miguel Alan Mora expresa que el Alcalde tiene la potestad de contratar a un informático externo y supervisar.

El Alcalde Municipal Luis Alberto Villalobos Artavia expresa que la funcionaria Yarline, no tiene contrato y hace cosas, a como lo dijo Gustavo.

El Ing. Gustavo Torres expresa que no todo el tiempo hace cosas Yarline, es de vez en cuando y es cuando el internet no funciona, pero los sistemas siempre funcionan.

Además, existen rastros, que detectan si algo se modifica, en el caso del departamento de informática, no puede modificar nada.

El Regidor Miguel Alan Mora expresa que no está bien que ese departamento sea unipersonal, que solo el informático tenga acceso a todo.

El Ing. Gustavo Torres responde que la Municipalidad no tiene presupuesto para compra un software.

El Presidente Municipal Juan Luis León Barrantes pregunta que al ser unipersonal este departamento ¿Qué pasa si el día de mañana Gustavo no está; por cualquier razón?

El Regidor Suplente Anthony Fallas Jiménez expresa, que el departamento de Auditoria; puede solicitar información al departamento de Informática, igual que el Alcalde Municipal.

El Ing. Gustavo Torres expresa que si existieran anomalías, su función es no decirlas, ya que eso es una función de un auditor investigar.

Además, el Alcalde puede pedir información y fiscalizar, este proyecto de reglamento no está escrito en piedra, pero la Contraloría General de la República se lo está solicitando, donde estuvo un año en el Departamento Legal de la Municipalidad y ya lo observo el Alcalde y hasta el Señor Luis Francisco Montoya, o sea ya paso por tres filtros.

El Alcalde Municipal responde que el Señor Luis Francisco Montoya no estaba contrato para eso.
El Ing. Gustavo Torres expresa que el Programa del SIIM, es funcional, pero ya está obsoleto.
El Alcalde Municipal le pregunta a Gustavo ¿que si desde una casa ese programa se puede ver?
El Ing. Gustavo Torres responde que es un sistema local y afuera no se pude ver.
Pero en el caso de la Funcionaria Tatiana, que es la Administradora del sistema y quiere llevarse una copia para trabajar en la casa lo puede hacer, luego se actualiza.
El Alcalde Municipal expresa que como Alcalde debería de informarle cuando algún funcionario se lleva el trabajo para la casa, ya que no se lo comunican.
El Regidor Luis Ángel Trejos Solís pregunta a Gustavo que si él puede ver el sistema desde la casa?
El Ing. Gustavo Torres expresa que es un sistema local, pero tiene acceso desde su computadora de la casa y celular, para corroborar en las mañanas si los servidores están encendidos, ya que a las siete de la mañana, se debe de garantizar que el sistema debe de funcionar y los sábados y domingos los revisa; porque son herramientas, los tiene que monitorear, está ligado a su correo electrónico y su correo al servidor.
El Regidor Luis Ángel Trejos Solís le pregunta a Gustavo ¿que existen rumores, que una persona que no tiene que ver nada con la Municipalidad, está manejando el sistema desde afuera y usted es el único que puede responder, ya que es una molestia general?.
El Ing. Gustavo responde que una copia puede verse, desde su casa. Y que la otra pregunta es falsa, porque es un programa local.
Que inclusive el correo electrónico del Alcalde anterior se lo quito y se enojo. Ya que para ver información desde afuera tiene que pedirlo.
No se puede tener acceso, así son las herramientas, tiene que hacerlo como un usuario y queda guardado, cualquier movimiento. Eso es seguridad de la información. Es un chisme y por un chisme no se pude despedir a nadie.

La Regidora Bernarda Agüero Alpizar expresa que si el Informático se percata de alguna anomalía, debería de comunicar.

El Ing. Gustavo responde que eso debería de ir en el manual de puestos. Y si es el caso que quisiera un estado diario, de las acciones que se hicieron por día, se lo pueden pedir. Pero no explicarles porque no tiene el conocimiento de muchas cosas, de lo que se hace en cada departamento.
Además hay tipo información como el respaldo al SIIM, egresos y los datos son locales, hay dos servidores uno para programar las tareas, a cierta hora se activa y replica para el otro servidor de datos, que es local.
La Regidora Bernarda Agüero Alpizar pregunta que si duplican una factura y no se investiga, ahí murió todo? Y que tanto peca el que hace, como el que deja de hacer.
El Ing. Gustavo Torres responde que el registro queda, se puede accesar, pero hay muchas cosas que desconoce de otros departamentos.
El Regidor Anthony Fallas Jiménez expresa que la Auditoria es la persona capacitada, la que tiene el conocimiento y la competencia para investigar cualquier anomalía. No es el Informático, ya que es una función del Auditor.
La Regidora Bernarda Agüero Alpizar expresa que el informático puede cumplir su labor y que el Alcalde le pida informes.
El Ing, Gustavo Torres expresa que el análisis de los informes seria con cada departamento.
El Ing. Gustavo Torres expresa que aquí se genera estados diarios, no sé porque no le llegan al Alcalde.
El hecho de que carecemos de reglamentos, muchos funcionarios no se hacen responsables de muchas cosas.
La Regidora Bernarda Agüero Alpizar expresa que como funcionario debe de respaldarse con sus hechos, porque como si reciben el salario. Lo cual deja mucho que decir de los profesionales.
El Regidor Suplente Anthony Fallas Jiménez expresa que con el afán de aumentar controles; el departamento de informática viene a explicarnos este reglamento.
Pero la fiscalización de las acciones; es función del auditor y no de este departamento, ya que este departamento no tiene conocimiento de las funciones de otros departamentos. Y los demás departamentos, pueden n venir a presentar sus reglamentos; a como lo está haciendo el informático.

El Regidor Miguel Alan Mora expresa que no le parece de que el hecho que no haya reglamento; se diga que no hay responsabilidades.
El Regidor Suplente Anthony Fallas Jiménez expresa que lo que quiere entender Gustavo, es que cada departamento tenga su propio reglamento.

ENTERADOS

INCISO Nº3:

El Presidente Municipal somete a votación para ampliar la sesión en media hora más.
RECHAZADA DE UNA FORMA UNANIME.

ENTERADOS

CAPITULO TERCERO- CIERRE DE SESION

INCISO Nº4: SIENDO LAS DIECISINUEVE HORAS Y TREINTA MINUTOS, EL SEÑOR PRESIDENTE JUAN LUIS LEON BARRANTES DA POR CONCLUIDA LA SESION.

PRESIDENTE MPL	**SECRETARIA MPL**