POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN LA ALCALDÍA DE RÍO DE ORO, CÉSAR

KATHEDRIN SÁNCHEZ ARIAS
Esp. YESENIA ARENÍZ ARÉVALO
Facultad de Ingenierías
Plan de Estudios de Ingeniería de Sistemas
Universidad Francisco de Paula Santander Ocaña
ksancheza@ufpso.edu.co

Fecha de recepción: 17 de septiembre de 2014
Fecha de aprobación: 22 de octubre de 2014

RESUMEN
Las Alcaldías son entidades del estado, del orden territorial y al servicio de la comunidad, cuyo objetivo es brindar programas de educación, salud, bienestar, servicios públicos y protección; de los cuales se maneja gran cantidad de información confidencial, que de no estar segura, generaría una mala imagen institucional, inconsistencias y pérdidas.

Para definir el nivel de seguridad en la Alcaldía, se realizó una investigación mediante la aplicación de encuestas dirigidas a su personal de planta y OPS, con el fin determinar el nivel de efectividad de los controles que actualmente aseguran la información manejada por ésta.

Como se demuestra en la investigación realizada, la vigilancia se mantiene solo en las horas de la noche, no se realiza controles en los horarios laborales, accesos del personal y visitantes, no se registra el uso de los sistemas, documentos institucionales y servicios, ni se investigan las incidencias ocurridas. Además, algunas áreas carecen de identificación, alarmas, cámaras, detectores de humo o extintores y de la prohibición del consumo de alimento y bebidas, o de fumar, entre otras.

Tras el análisis de las necesidades presentes, se recomienda aplicar las Políticas de Seguridad de la Información ajustadas a la Alcaldía, para fomentar el compromiso de uso.

PALABRAS CLAVES
Alcaldía, análisis de riesgos, ISO/IEC 27002, seguridad de la información.

ABSTRACT
Mayors are entities of state, territorial order and serving the community which aim to provide education, health, welfare, public services and protection; with a large amount of confidential information that generates a poor corporate image, inconsistencies and losses are handled.

To define the level of security at Mayor, an investigation was carried out by applying one survey of plant personnel and OPS, to determine the level of effectiveness of controls to ensure the information currently managed by this.

As demonstrated in the investigation, surveillance is maintained only in the evening hours, no controls on working hours, access for staff and visitors is performed, the use of systems, institutional documents and services is not recorded, nor investigated the incident occurred. In addition, some areas is missing about identification, alarms, cameras, smoke detectors, fire extinguishers and the prohibition of the consumption of food and beverages, or smoking, among others.

After analyzing the present needs, it is recommended to apply the Policy Information Security tight for Mayor, fostering commitment of Use.

KEY WORDS
Analysis of risks, Governorship, ISO/IEC 27002, information security.

INTRODUCCIÓN
La seguridad informática siempre ha sido importante, desde los inicios de los computadores. Pero ahora se ha agudizado más la importancia de contar con buenos mecanismos de seguridad debido a que los riesgos y amenazas no solamente consisten en que personas en el área de equipos roben información, sino que ahora también existen riesgos de robo o accesos no autorizados a información mediante las diferentes redes que interconectan a los computadores o a cualquier equipo tecnológico utilizado para transmitir información digital.

Aunque muchas entidades públicas y privadas le restan valor o importancia a este aspecto, no hay duda de que las pérdidas por la falta de seguridad pueden ser realmente caras, tanto en materia económica como en prestigio o problemas legales, entre otros.

En vista de la importancia que tiene la seguridad en las tecnologías de la información, no es suficiente estudiar buenas prácticas y consejos sabios de personas que llevan una gran trayectoria en el área de la informática, sino que más aún, las

normas internacionales certificables son un gran beneficio para cualquier organización. Por esto, la adopción de la Norma Internacional ISO/IEC 27002 es totalmente beneficiosa para cualquier entidad que tenga que ver de alguna forma con la seguridad de las tecnologías de la información, mediante la implementación de acciones y procedimientos necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información.

La Organización Internacional de Normalización (ISO) y La Comisión Electrotécnica Internacional (IEC), se unieron para crear lineamientos de seguridad, que se ajustan a los objetivos de las organizaciones, los cuales se encuentran consagrados en un documento titulado "Política de Seguridad de la Información" referenciado como la norma internacional de buenas prácticas ISO/IEC 27002, compuesta por 39 objetivos de control y 133 controles, agrupados en 11 dominios. Esta política cuenta con una serie de lineamiento de implementación que definen el tema, sus objetivos, alcances e importancia, estructuras de evaluación y gestión de riesgos, entre otros.

Es importante traer a cuento que ningún conjunto de controles puede lograr la seguridad completa, pero sí puede reducir al máximo los riesgos que amenacen con afectar la seguridad en una organización; por lo que las políticas de seguridad de la información deben ser continuamente revisadas y actualizadas para que se mantengan en condiciones favorables y en concordancia con los cambios tecnológicos y demás, que se den a través del tiempo.

El documento de la política de seguridad de la información, debe ser creado de forma particular por cada organización, aprobado por la administración y luego publicado y comunicado a todo el personal y las partes externas relevantes. Pero no antes de realizar un análisis de riesgos y controles actualmente aplicados, que definan los lineamientos a implementar, para minimizar los riesgos a los cuales se encuentra expuesta la información en la actualidad.

Para el caso, la Alcaldía Municipal de Río de Oro (Cesar) está conformada por cuatro Secretarías, las cuales brindan apoyo al alcalde en los diferentes programas. Éstas son: Secretaría de Gobierno, Planeación, Hacienda y Salud, de las cuales dependen oficinas como: la Comisaría de Familia, la Inspección de Policía, la Coordinación de Cultura, Deporte y Recreación, La Coordinación Ambiental, de Salud Pública, de Promoción Social, La Coordinación del SISBEN y de Gestión de Banco de Proyectos. Además existen oficinas destinadas al apoyo de Los Programas de Más Familias en acción, Adulto Mayor y Victimas.

MATERIALES Y MÉTODOS

Con el fin de determinar, en qué medida es necesaria la aplicación de Políticas de Seguridad de la Información en la Alcaldía de Río de Oro, Cesar, se realizó una investigación que buscaba calcular el nivel de aplicación y de efectividad de los controles de seguridad de la información en ésta; usando como técnica, una encuesta dirigida a 21 de los 31 empleados que componen el organigrama, distribuidos en 13 empleados de planta y 8 OPS, con el propósito de lograr un paralelo entre ellos.

Se empleó el tipo de investigación descriptiva, ya que se refirieron las características de la situación actual en la Alcaldía, mediante representaciones gráficas, asociadas a los cuestionarios realizados.

RESULTADOS

A continuación se reflejan y detallan los resultados de la investigación anteriormente descrita.Por parte de los Empleados de Planta:

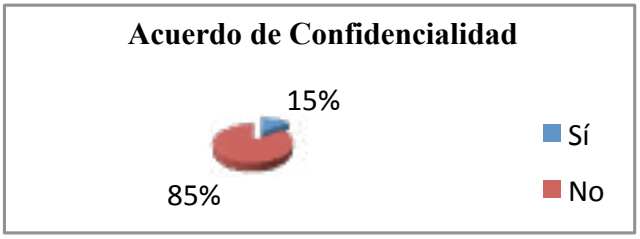


Figura 1. Acuerdo de Confidencialidad

En la figura 1 se observa que el 85% de los encuestados no cuenta con un acuerdo de confidencialidad de la información, de los cuales poco más de la mitad, no conoce sus responsabilidades y sanciones, frente a la seguridad de la información, mientras que el 15% restante, cuenta con pleno conocimiento de estas, de decretos o resoluciones institucionales.

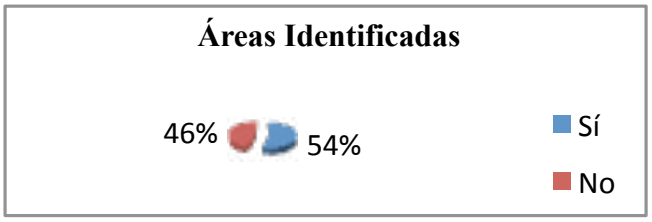


Figura 2. Áreas identificadas

Como evidencia la figura 2, el 54% de los empleados afirma que el área en la cual labora se encuentra debidamente identificada, mientras que el 46% afirma que no lo está, lo que provoca que los visitantes no encuentren el área de la cual requieren el servicio, creando retrasos y una mala imagen institucional.

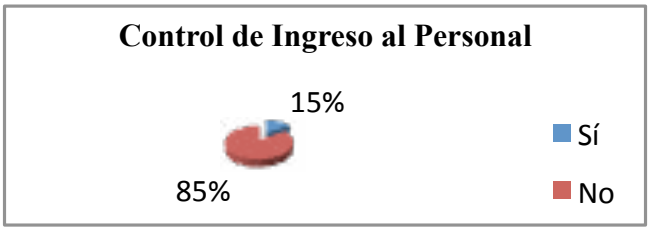


Figura 3. Control de Ingreso al Personal

El ingreso del personal no es controlado en un 85%, así con el trabajo fuera del horario laboral definido, por la administración. (Ver figura 3).

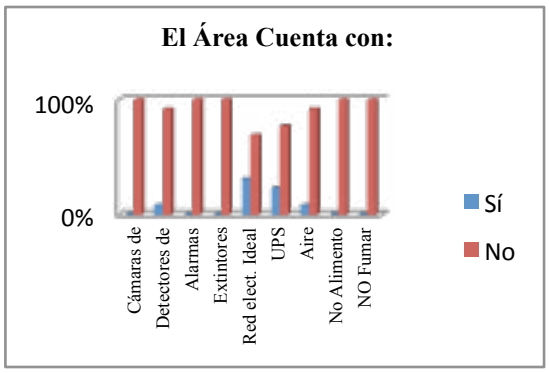


Figura 4. El Área Cuenta con

En la figura 4 se observa que ninguna de las áreas cuenta con cámaras de vigilancia, alarmas o extintores, y sólo el 8% cuenta con detectores de humo, lo que implica un riesgo importante en la Alcaldía.

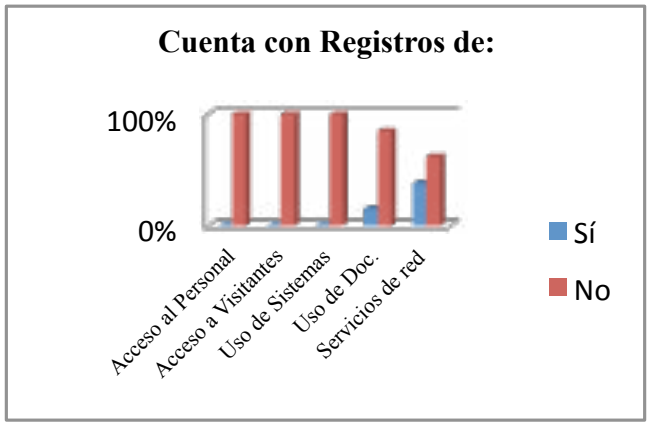


Figura 5. Cuenta con Registros de.

La Alcaldía no cuenta con el registro de acceso a sus instalaciones del personal y los visitantes, ni del uso de los sistemas por alguien distinto al empleado en específico. Además, el uso de los documentos institucionales sólo se registra en un 15% y el uso de los servicios de red en un 38%. (Ver figura 5).

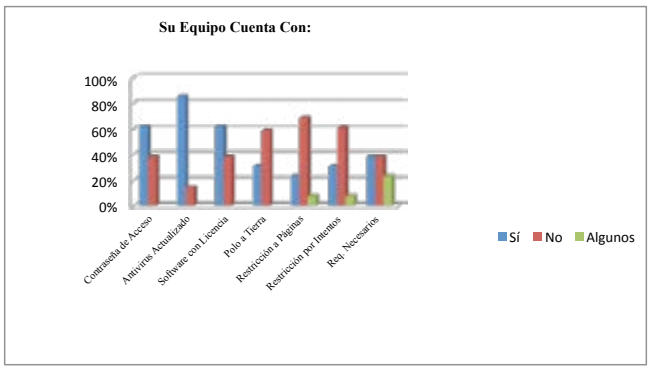


Figura 6. Su Equipo Cuenta con

Como se ve en la figura 6, el 62% de los equipos cuenta con una contraseña para permitir el acceso de usuarios a los sistemas. Por su parte, el 85% de éstos, mantiene el antivirus actualizado, el 62% cuenta con su software licenciado e indistintamente el 59%, carece de polo a tierra.

Las restricciones de acceso a páginas web (redes sociales, etc.) en los equipos de los empleados encuestados, es del 23% para todas, del 69% para ninguna y el 8% para algunas de las mismas.

Por otra parte, el acceso restringido a las aplicaciones después de varios intentos es usado en el 23% de los equipos, nulo en el 61% y parcial en el 8%. Además, el 38% de los encuestados consideran que su equipo cuenta con los requerimientos necesarios para la realización óptima de sus labores, al igual que una misma fracción de estos considera que no, pero indistintamente un 8%, considera que cuenta con solo algunos de estos requerimientos.

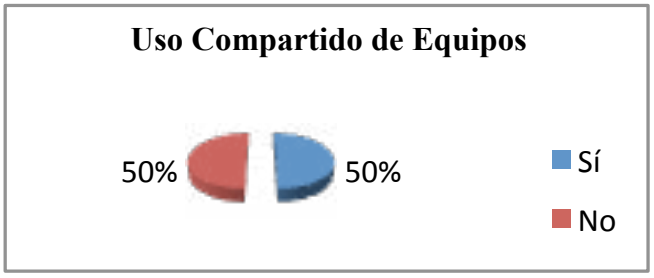


Figura 7. Uso compartido de Equipos

La figura 7 muestra que el 50% de los equipos es usado por alguien además del encuestado, una situación que contrasta con la seguridad de la información.

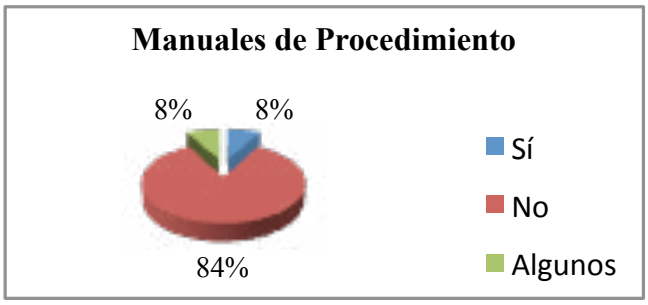


Figura 8. Manuales de procedimiento

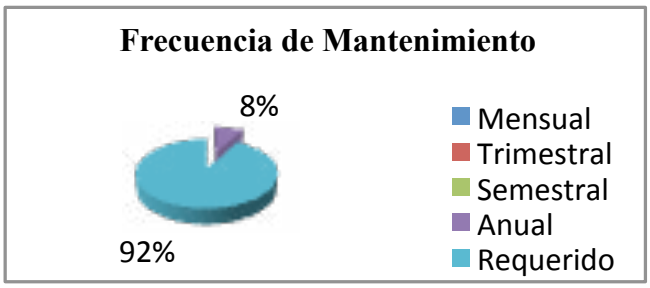


Figura 9. Frecuencia de Mantenimiento.

En cuanto a la frecuencia con la que los equipos a disposición de los encuestados, recibe mantenimiento, vemos que es del 92% cuando éste lo requiere y el 8% anualmente. Es indudable la falta de mantenimiento preventivo que reciben estos equipos, poniendo en riesgo la información en las áreas. (Ver figura 9).

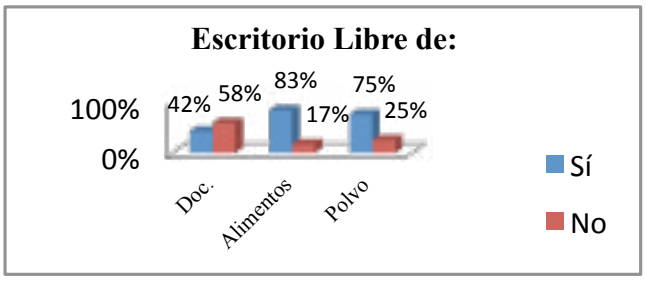


Figura 10. Escritorios limpios.

En lo referente a la política de escritorios limpios, el 58% de los empleados afirma que su escritorio no permanece libre de archivos o documentos institucionales.

El 83% de ellos mantiene su escritorio libre de alimentos y el 75%, libre de polvo. (Ver figura 10).

Se puede percibir que hay un nivel de cultura entre los funcionarios a cerca de la importancia de cuidar los equipos ante los inminentes riesgos de la cotidianidad, pero se debe mejorar aún más.

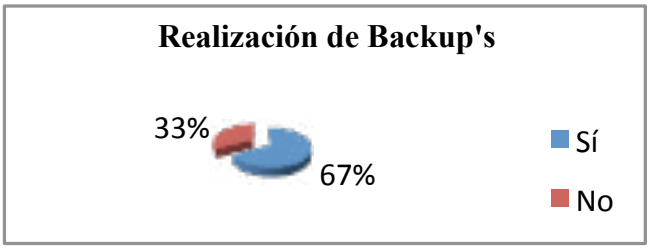


Figura 11. Realización de Backup's.

La figura 11 muestra que el 33% de los encuestados no realiza Backup's (Copias de Seguridad) de la información a su disposición, mientras que el otro 67% prefiere almacenar sus backup's en memorias USB, discos duros o imprimirlas, a través de un proceso realizado con una periodicidad diaria, semanal y hasta mensual.

En cuanto al almacenamiento de Backup's, los encuestados prefieren resguardar su información en estantes o gavetas, muebles con cerradura o archivadores, y en algunos casos en un sitio fuera de las instalaciones de la Alcaldía, para prevenir la pérdida de datos en caso de incidencias.

En ese sentido y debido a que la información debe mantenerse segura, gran parte de los encuestados opina que el acceso a las copias de respaldo o documentos institucionales es restringido, según el rol del funcionario dentro de la Alcaldía y su solicitud puede realizarse de forma verbal o escrita.

Aunque la Alcaldía es un establecimiento público, que debe brindar la disponibilidad de la información ante la solicitud del interesado, existe cierta información que debe ser confidencial para evitar episodios que pongan en peligro su integridad. Por tal razón, los encuestados concuerdan en que cierta información no debe ser divulgada y que su solicitud en la mayoría de los casos debe realizarse de forma escrita.

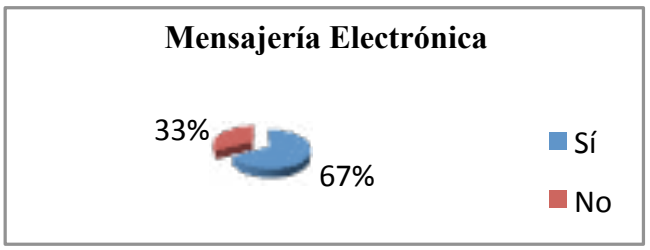


Figura 15. Mensajería Electrónica

Los empleados no cuentan con ningún tipo de aplicación que les permita encriptar su información de destinatarios no deseados, confiando en los controles de seguridad que practican los proveedores de correo electrónico. Sin embargo, el uso de mensajería electrónica es del 67%. Así mismo no cuentan con un procedimiento formal para reporte de incidentes (robos de información, pérdida de datos, accesos no permitidos, etc.), de los que hasta el momento no se realizan investigaciones, ni recolección de evidencias. (Ver figura 12).

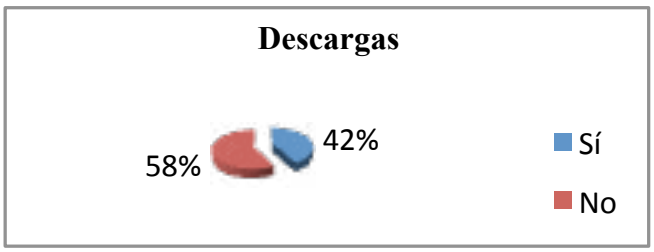


Figura 13. Descargas

El 42% de los encuestados realiza descargas de música, películas, programas entre otros, lo que pone en riesgo la seguridad de la información a su cargo, debido a los virus informáticos. (Ver figura 13).

Por parte de los Empleados OPS:

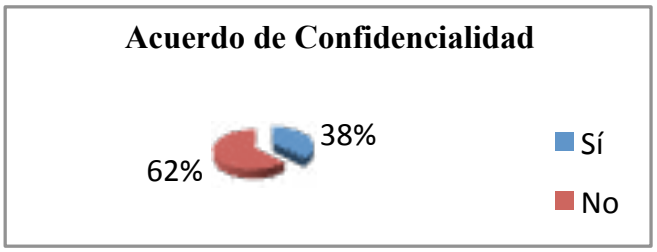


Figura 14. Acuerdo de Confidencialidad

En la figura 14, se observa que el 62% no cuenta con un acuerdo de confidencialidad de la información, la mitad de ellos no tiene conocimiento de sus responsabilidades y sanciones, frente a la seguridad de la información, mientras que los demás, cuentan con pleno conocimiento de dicha normatividad.

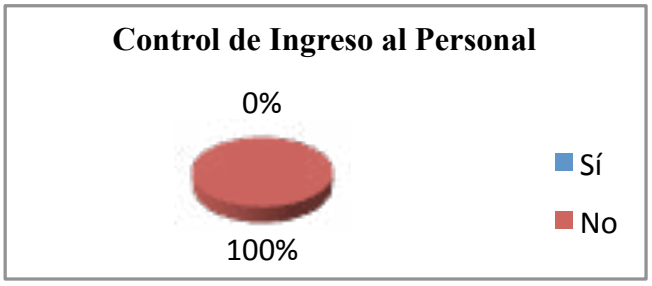


Figura 15. Control de Ingreso al Personal

Al personal no se le controla el acceso al igual que su trabajo fuera del horario laboral definido, por la administración, tal como lo evidencia la figura 15.

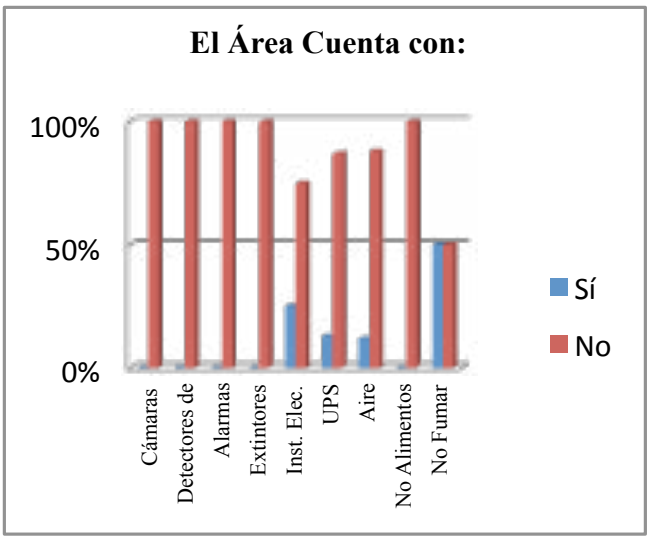


Figura 16. Recursos de áreas

En la figura 16, se observa que ninguna de las áreas de trabajo de los empleados OPS cuenta con cámaras de vigilancia, detectores de humo, alarmas o extintores.

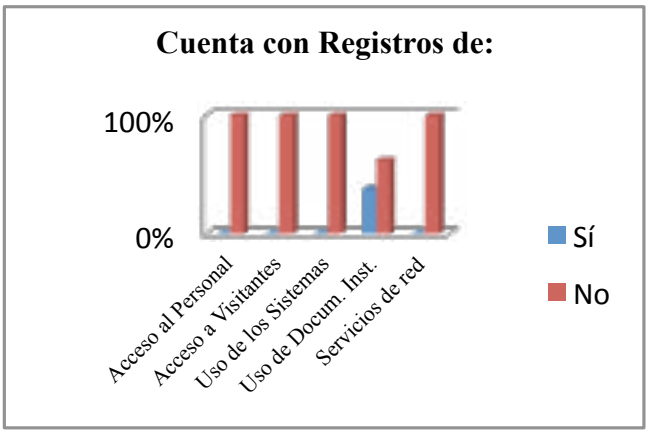


Figura 17. Registros

En la figura 17, se aprecia que la Alcaldía Municipal no cuenta en su totalidad con el registro de acceso a sus instalaciones del personal y los visitantes, ni del uso de los sistemas por alguien distinto al empleado en específico.

Además, el uso de los documentos institucionales sólo se registra en un 38%, y el uso de los servicios de red en un 0%.

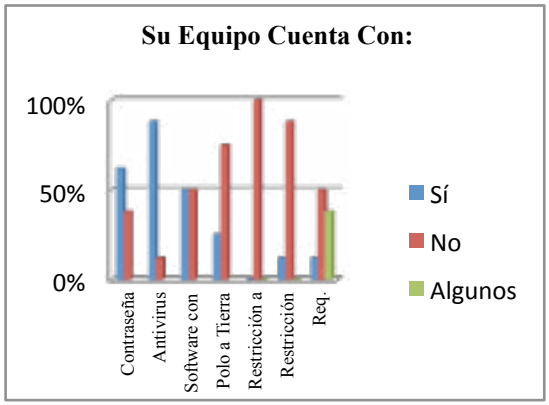


Figura 18. Recursos en equipos

En lo relacionado con los controles de seguridad de la información aplicados en cada equipo, cabe mencionar que el 62% de los equipos de los empleados encuestados cuenta con una contraseña (para permitir el acceso de usuarios a los sistemas), mientras que el 88% de éstos, mantiene el antivirus actualizado. Además, el 50% cuenta con su software licenciado e indistintamente el 25%, carece de polo a tierra. (Ver figura 18).

Las restricciones de acceso a páginas Web (redes sociales, etc.) en los equipos de los empleados encuestados son del 0% para todos, del 100% para ninguna y el 0% para algunas de éstas.

Por otra parte, el acceso restringido a las aplicaciones después de varios intentos es de total uso en el 12% de los equipos, nulo en el 88% y parcial el 0%.

Además, el 12% de los encuestados considera que su equipo cuenta con los requerimientos necesarios para la realización óptima de sus labores, pero el 50% de éstos considera que no, indistintamente un 38%, considera que cuenta con sólo algunos de estos requerimientos.

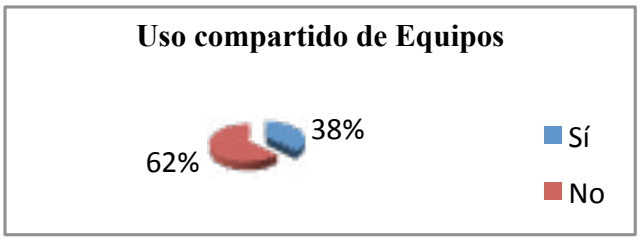
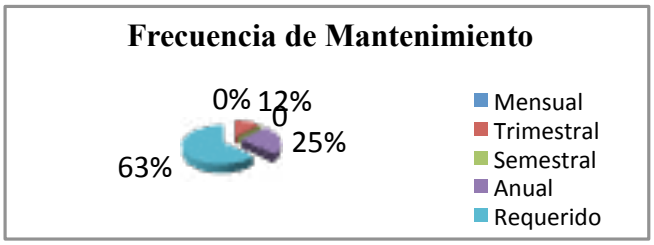


Figura 19. Uso compartido de Equipos

A diferencia de los empleados de planta, en los empleados con contrato OPS, el número se incrementa a un 67% de aquellos para quienes el uso de su computador es exclusivo. (Ver figura 19).



Como se ve en la figura 20, la frecuencia con la que los equipos a disposición de los encuestados recibe mantenimiento, es del 63% cuando éste lo requiere, el 25% anualmente y el 12% trimestralmente. En los que tienen contrato OPS existe al menos un pequeño porcentaje de mantenimientos que se hacen de forma preventiva, aunque el número debería ser mayor.

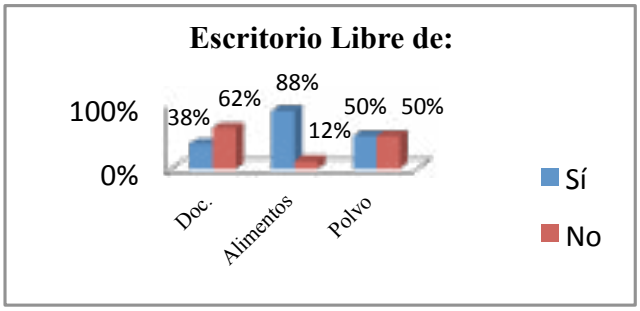


Figura 21. Escritorios limpios

En lo referente a la política de escritorios limpios, el 38% de los empleados afirma que su escritorio permanece libre de archivos o documentos institucionales.

El 88% de ellos mantiene su escritorio libre de alimentos y el 50%, libre de polvo. (Ver figura 21).

Frente a los empleados de planta, hay una mayor cultura de los elementos que pueden afectar los equipos, pero es necesario se siga trabajando en este aspecto.

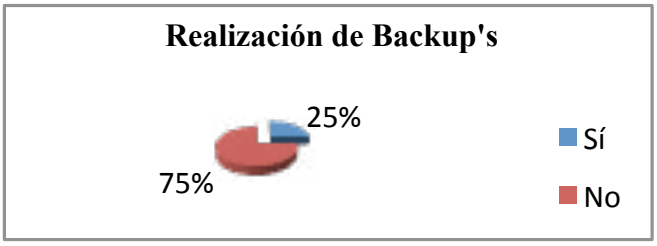


Figura 22. Realización de Backup's

La figura 22 muestra que el 75% de los encuestados no realiza Backup's (copias de Seguridad) de la información a su disposición, mientras que el otro 25% prefiere almacenar sus backup's en memorias USB, discos duros o imprimirlas.

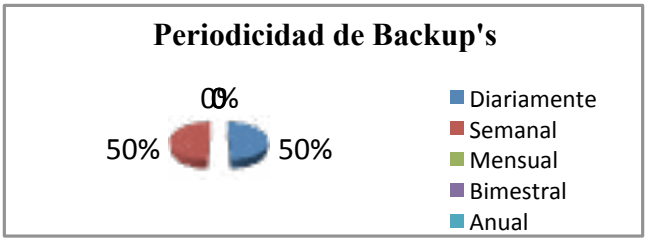


Figura 23. Periodicidad de Backup's

En la figura 23, se observa que los empleados encuestados realizan sus backup's con una periodicidad diaria en un 50%, mientras que semanalmente estos procesos se realizan en el 50% restante, convirtiéndose en un ejercicio apropiado para la seguridad de la información.

En cuanto al almacenamiento de Backup's, los encuestados prefieren resguardar su información en estantes o gavetas.

Debido a que la información debe mantenerse segura, el 100% de los encuestados opina que el acceso a las copias de respaldo o documentos institucionales es restringido, según el rol del funcionario dentro de la Alcaldía y su respectiva solicitud de acceso debe realizarse de forma verbal o escrita, depende el caso.

Los encuestados concuerdan en opinar que la información confidencial no sea divulgada.

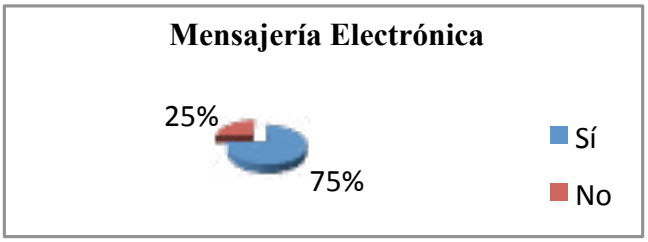


Figura 24. Mensajería Electrónica

Como se evidencia en la figura anterior, un gran porcentaje (75%), hace uso de la mensajería electrónica, pero no cuentan con ningún control adicional al que suministra el proveedor.

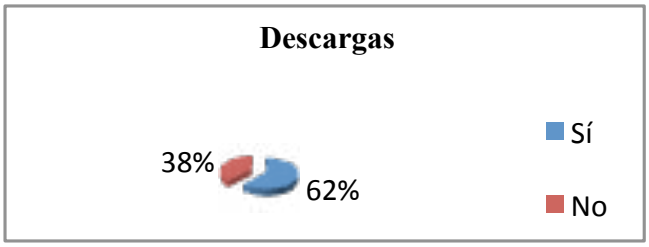


Figura 25. Descargas.

El 62% de los encuestados realiza descargas de música, películas, programas entre otros, lo que pone en riesgo la seguridad de la información a su cargo, debido a virus al descargar.

El 62% de los encuestados realiza descargas de música, películas, programas entre otros, lo que pone en riesgo la seguridad de la información a su cargo, debido a virus al descargar.

RECOMENDACIONES

Tras el análisis de los resultados obtenidos en esta investigación, se recomienda:

- Realizar el respectivo control de los horarios laborales de los empleados.
- Realizar el registro de accesos del personal y los visitantes a las instalaciones.
- Realizar el registro de uso de los sistemas, documentos institucionales y servicios.
- Implementar planes de contingencia y realizar la respectiva investigación de incides ocurridos.
- Contar con vigilantes las 24 horas del día.
- Realizar la respectiva y correcta identificación de la totalidad de las áreas pertenecientes a la Alcaldía.
- Contar con una recepcionista para las áreas con mayor flujo de personas.
- Instalar alarmas, cámaras de vigilancia, aire acondicionado, detectores de humo y extintores en áreas estratégicas, además de contar y mantener cargadas las UPS´s necesarias.
- Prohibir el consumo de alimentos y bebidas, así como fumar en el área de trabajo o cerca a los equipos.
- Contar con acuerdos de confidencialidad físicos, que describan sus responsabilidades y sanciones, en caso de provocar la violación a la seguridad de la información a su disposición.
- Contar con manuales de procedimiento necesarios para la operación de los sistemas de su área.
- Realizar copias de respaldo de la información a su cargo, para evitar la pedida de la misma.
- Permitir el acceso a los documentos institucionales solo a personas autorizadas.
- Realizar comunicaciones electrónicas, solo por medios seguros.
- Evitar al máximo la descarga de archivo, a menos que sea de una página considerablemente segura.
- Mantener una contraseña de acceso, de tipo alfanumérico, con mínimo 10 caracteres, no deducible y cambiada regularmente.
- Mantener el software (sistema operativo, antivirus, programas, etc.) con sus respectivas licencias y actualizado (preferiblemente últimas versiones o al menos que aún mantengan soporte del proveedor).

- Restringir el acceso a páginas Web, que comprometan la seguridad de la información.
- Establecer restricciones de acceso por contraseña luego al menos tres (3) intentos erróneos.
- Contar con los requerimientos necesarios para la realización optima de las labores diarias de los empleados.
- Evitar al máximo que los equipos sean usados por más de una (1) persona.
- Contar con polo a tierra, evitar accidentes.
- Establecer planes de mantenimiento continuo.

CONCLUSIONES

A través de la investigación realizada, sobre los controles de seguridad de la información que actualmente se lleva a cabo, en la Alcaldía Municipal de Río de Oro (Cesar), se puede concluir que: su información es propiedad del municipio y requiere una protección especial que garantice su preservación así como su integridad, confidencialidad y disponibilidad.

A modo de consideraciones, se recomienda: aplicar las Políticas de Seguridad de la Información ajustadas a la Alcaldía, además de fomentar el compromiso en los empleados con la aplicación de los controles allí consagrados.

BIBLIOGRAFÍA

ERB, Markus. Gestión de Riesgo en la Seguridad Informática. Amenazas y Vulnerabilidades. España. 3h. [en línea]. http://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

Governance Institute. Oficina gubernamental de comercio. The Stationery Office. Alineando COBIT 4.1, ITIL V3 e, ISO/IEC 27002 en beneficio del negocio. Estados Unidos e Inglaterra. 2010. 130h. [en línea]. Extraído de: http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-Cobit-4.1,-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa-v2,7.pdf.

Ministerio de la Información y las Comunicaciones. Reglamento sobre Seguridad Informática. La Habana. Cuba. 2012. 15h. Extraído de: http://fcmfajardo.sld.cu/seguridad_informatica/resol_y_dispos_del_mic/reglamento_seguridad_informatica.pdf

Ministerio del Interior y de Justicia de Colombia. Dirección Nacional del Derecho de Autor. Unidad Administrativa Especial. Extraído de: http://www.propiedadintelectualcolombia.com/Site/LinkClick.aspx?fileticket=yDsveWsCdGE%3D&tabid=

Presidencia del Consejo de Ministros de Perú. Políticas de Seguridad Informática a través de la Oficina de Gobierno Electrónico e Informático. Lima. Perú. 2013. 15h. Extrraído de: http://www.enterese.net/entidades-del-estado-se-modernizan-con-politicas-de-seguridad-informatica/

Superintendencias de Sociedades. Manual Manejo y Control Administrativo de los Bienes de Propiedad. Bogotá D.C., Colombia, 2009. 29h. Extraído de: http://www.supersociedades.gov.co/web/Ntrabajo/SISTEMA_INTEGRADO/Documentos%20Infraestructura/DOCUMENTOS/GINF-M-001%20MANUAL%20ADMINISTRATIVO.pdf

Francisco de Paula Santander Ocaña. Módulo Evaluación de la Seguridad de la Información. Ocaña. Colombia. 2012. 65h.

Universidad Libre. Acuerdo No. 05 (Noviembre 17 de 2009). Colombia. 2009. 85h. [en línea]. http://www.unilibre.edu.co/images/pdf/acd_05-09.pdf

Universidad Nacional Abierta y a Distancia.. Gerencia de Innovación y Desarrollo Tecnológico. Última actualización el Lunes, 22 de Abril de 2013 09:05. [en línea]. http://www.unad.edu.co/gidt/index.php/leyesinformaticas