Norte 08 de octubre de 2019
EKRM - 9134-19

Señor(es):
CAMARA DE COMERCIO DE SANTA MARTA PARA EL MAGDALENA
Atn: Dr. ALFONSO LUIS LASTRA FUSCALDO
Representante Legal
Ciudad.

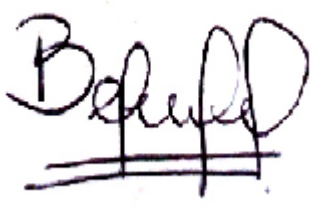
ASUNTO: MEMORANDO DE RECOMENDACIONES PARA FORTALECER LOS SISTEMAS DE INFORMACIÓN

Respetados Señores

Para su conocimiento y fines pertinentes, estamos enviando el memorando de recomendaciones para fortalecer las seguridades y controles en los sistemas de información.
Es prudente mencionar que nuestra labor se desarrolló de acuerdo con las normas de auditoría generalmente aceptadas en Colombia, utilizando los procedimientos y pruebas que aconseja la profesión y con base en pruebas selectivas, lo que hace que el cumplimiento de la auditoría no sea el cien por ciento de los aspectos relacionados con las seguridades y controles, sino una selección técnica de ellos. Por este motivo sería conveniente que la administración le diera un barrido al 100% de las actividades y operaciones de sistemas, especialmente a aquellos puntos en que llamamos su atención.

Las observaciones mencionadas en este informe, fueron socializadas con el Ingeniero Jorge Miranda Castellanos Coordinador de Infraestructura Tecnológica, Dr. Gabriel Barrios Martínez Jefe de Control Interno, Dra. Cindy Cabrales Jefe de Talento Humano y Servicios, Ingeniero Juan Pablo Llinas Ramírez Coordinador de Desarrollo e Innovación de las TICS.

Cordialmente,



BELKIS CECILIA RODRIGUEZ PÉREZ

Miembro en Colombia de AFG Union is strength
Miembro exclusivo para Colombia de KRESTON
A member of Kreston International A global network of independent accouting firms
Calle 72 # 10 - 07 Edif. Liberty Seguros Oficina 1103 Bogotá - Colombia PBX: 7443680 - Mercadeo: 466 1095
Carrera 35 A # 15B - 35 Ofc. 310 El Poblado. Centro de Negocios Prisma Tél: 3662639
Medellín, Antioquia - Colombia
Carrera 100 # 11 - 60 Loc. 227 C.C. Holguines Trade Center Teléfono 3729912 Fax: 3313154
Santiago de Cali, Valle del Cauca - Colombia
Email: rmrf@kreston.co
g.mercadeo@kreston.co
www.kreston.com.co
ISO 9001 icontec Internacional Código SC 6920-1
CERTIFIED IQNet MANAGEMENT SYSTEM

Gestor de Auditoría Informática

Kreston R.M S.A.
Consultores, Auditores, Asesores
Kreston Colombia
Miembros de Kreston International Ltd.

CC Archivo.

CAMARA DE COMERCIO DE SANTA MARTA PARA EL MAGDALENA
08 de octubre de 2019
Elaborado por: **Kreston RM S.A.**

INFORME GERENCIAL

Dentro de nuestra auditoría utilizamos un "check list" para la verificación de algunos aspectos vitales para la entidad. Algunos de estos aspectos se están cumpliendo y otros no. A los puntos válidos (cuya respuesta como resultado de nuestra auditoría es SI) se les asigna un porcentaje de cumplimiento dentro del total. Igualmente, de acuerdo con la tabla anotada, le consignamos un riesgo dependiendo del porcentaje asignado.

Así las cosas, les enviamos para su análisis el porcentaje y si desean ver en cuáles puntos se debe fortalecer pueden ver el cuerpo del informe.

Resumen cualificación total

Procedimiento	Calificación	Riesgo
A. CONOCIMIENTO GLOBAL DE LA ENTIDAD Y SUS RECURSOS TECNOLÓGICOS	%100	BAJO
B. CONTROL INTERNO	%86.66	BAJO
C. POLÍTICAS GENERALES	%89.74	BAJO
D. PÓLIZAS DE SEGUROS	%100	BAJO
E. SEGURIDADES FÍSICAS EN INSTALACIONES	%90.90	BAJO
F. CONTROL DE ACCESOS	%85	BAJO
G. ADMINISTRACIÓN DE INCIDENTES	%80	MODERADO
H. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	%80	MODERADO
B. RED DE DATOS	%88.88	BAJO
C. INTERNET	%100	BAJO
D. PROCEDIMIENTOS DE RESPALDO	%77.77	MODERADO
E. LICENCIAMIENTO DE SOFTWARE	%100	BAJO
F. ANTIVIRUS	%100	BAJO
G. CONTRATOS	%100	BAJO
H. PROYECTOS INFORMÁTICOS	%77.77	MODERADO
I. DESARROLLO DE SOFTWARE	%100	BAJO
J. COMUNICACIÓN DE ÁREA CON LAS OTRAS ÁREAS	%83.33	MODERADO
K. MANTENIMIENTO Y ASEO DE EQUIPOS	%93.33	BAJO

Convenciones

Requiere análisis e implementación urgentes (0 - 20%)	ALTO
Algunos Aspectos Necesitan Implementación (21 - 60%)	MEDIO
Implementado, requiere fortalecer algunos aspectos (61 - 84%)	MODERADO
Implementado y funcionando: requiere poca mejora (85 - 100%)	BAJO

CAMARA DE COMERCIO DE SANTA MARTA PARA EL MAGDALENA
08 de octubre de 2019
Elaborado por: **Kreston RM S.A.**

ASUNTO: MEMORANDO DE RECOMENDACIONES PARA FORTALECER LOS SISTEMAS DE INFORMACIÓN

B. CONTROL INTERNO

Actividad realizada

1 - Se observa que el Coordinador de Desarrollo e Innovación de las TICS, viene adelantando un documento de políticas de información, pero no están revisadas ni aprobadas por la Dirección General.

Sustento conceptual

1- De conformidad con los lineamientos de la Norma Técnica Internacional ISO IEC 27001:2013, frente al objetivo de control Políticas de Seguridad de la Información, las organizaciones deben contar frente a su red de datos con políticas escritas y debidamente aprobadas, en cuanto al uso y seguridad de la red de datos, así mismo estos lineamientos deben ser socializados a los usuarios con el fin de mantener un ambiente de seguridad.

2- De acuerdo a la Norma Internacional ISO IEC 27001:2013 en el control de Aspectos Organizativos de la Seguridad de la Información, hoy en día las organizaciones deben contar con asignación de roles y responsabilidades para atender los requerimientos y necesidades de los usuarios internos y externos.

Observaciones

1- Se evidencia que la Entidad no cuenta con normativa de uso de los sistemas de información.

2- Se observa que la Entidad cuenta con roles definidos pero sus responsabilidades no se encuentran especificadas de acuerdo a las funciones de cada cargo.

Riesgo

1- Se puede presentar:

- Imposibilidad de tener lineamientos claros en materia de seguridad de la información.
- Pérdida de información.

2- Incumplimiento en los requerimientos de los usuarios, pérdida de información sensible de la Entidad.

Oportunidad de mejora

1- Se sugiere documentar e implementar, y socializar con todos los usuarios una Normativa de Seguridad de la Información y los procedimientos correspondientes, que incluya uso y seguridad de la red de datos, intercambio de información, gestión de activos, seguridad física, gestión de incidentes, entre otros.

2- Se sugiere implementar un documento que definida específicamente los roles y responsabilidades de cada funcionario del área de sistemas.

C. POLÍTICAS GENERALES

Sustento conceptual

1- De acuerdo a la Norma Internacional ISO IEC 27001:2013 en el control de Organización de la Seguridad de la Información, las organizaciones deben definir indicadores del área presupuestal para medir las ejecuciones de los diferentes proyectos del área de sistemas.

2- De conformidad con los lineamientos de infraestructura tecnológica de información ITIL, en el objetivo de control referente a la Gestión de Seguridad de la Información, las organizaciones deben contar con una planeación a corto, mediano y largo plazo, que permita establecer las actividades, proyectos, mediante unos indicadores se realice un seguimiento para que se cumplan.

3- De acuerdo a la Norma Internacional ISO IEC 27001:2013 en el control de organización de la seguridad de la información, las organizaciones deben definir de forma clara todas las responsabilidades, funciones, procedimientos para cada puesto de trabajo dentro del área de sistemas.

4- Conforme a lo indicado en el Estándar Internacional COBIT (Control de Objetivos para Tecnologías de Información y Relacionadas, en inglés: Control Objectives for Information and related Technology), en el objetivo de control Análisis de Riesgos. Las organizaciones deben contar con análisis de riesgos asociados a sus sistemas de información, permitiendo tener claridad sobre sus riesgos latentes, así como

los controles que los mitigan.

Observaciones

1- La Cámara de Comercio no cuenta con indicadores de gestión que midan la ejecución de presupuestos para proyectos informáticos, y demás cosas inherentes que tenga que ver con el área de sistemas.

2- Se evidencia que la Entidad no cuenta con una planeación a corto, mediano y largo plazo, para el área de sistemas.

3- No se cuenta con manual de procedimientos de funciones y responsabilidades para cada puesto de trabajo del área de sistemas.

4- Se observa que la Empresa aun no cuenta con una matriz de riesgos y controles para el área de tecnología, para su correspondiente análisis e identificación.

Riesgo

1- Incumplimiento en las entregas y monitoreo de los proyectos próximos a realizar.

2- Se puede presentar:

- Incumplimiento de las actividades programadas en el plan de acción.
- Falta de coordinación entre los diferentes procesos.

3- Incumplimiento en la atención de los requerimientos en el área de sistemas.

4- Se puede presentar:

- Falta de claridad de cómo actuar en situaciones o problemas que se puedan presentar frente a los sistemas de información.
- Falta de conocimiento sobre los riesgos que posee la Organización en sus sistemas de información.

Oportunidad de mejora

1- Se recomienda crear e implementar indicadores que midan eficazmente las ejecuciones de los presupuestos de los proyectos a realizar, para mitigar los incumplimientos en las entregas y el proceso de monitoreo sea eficaz.

2- Se recomienda diseñar e implementar cada año un plan de actividades, proyectos, tiempos de ejecución para el área de tecnología con sus respectivos recursos asignados, en este caso ya para el año 2020.

3- Se recomienda documentar, aprobar e implementar las asignaciones de las funciones del personal del área de sistemas.

4- Se sugiere la implementación de la matriz de riesgos, donde muestre los diferentes escenarios de riesgos asociados al área de tecnología con sus respectivos controles de mitigación.

D. PÓLIZAS DE SEGUROS

Actividad realizada

1 - La Entidad cuenta con una Póliza Multiriesgo Empresarial con la entidad Seguros comerciales bolivar, con No.1512-3050153-01 y cobertura total, con una vigencia hasta el 22 de febrero del año 2020.

E. SEGURIDADES FÍSICAS EN INSTALACIONES

Actividad realizada

1 - Se observa que la Organización tiene por sectores cámaras de vídeo vigilancia como son: el área de caja, recepción y entrada; posee en el centro de datos en la entrada un lector de huellas, como en otras dependencias para llevar a cabo el control solo del personal autorizado.
También encontramos que las alarmas contra intrusos se encuentran por sectores: Dirección Financiera, Centro de Desarrollo Empresarial, Talento Humano.

2 - Se pudo observar que se cuenta con señalización, en caso de una emergencia en los alrededores de los pasillos de las oficinas de la Entidad.

3 - El personal encargado del área de sistemas que son: el Coordinador de Infraestructura Tecnológica y el Coordinador de Desarrollo e Innovación, manifiestan que están en pocos días a trasladarse a una nueva sede, por lo cual algunos equipos están desorganizados y desarmados en el centro de datos.

Sustento conceptual

1- De acuerdo a la Norma Técnica ISO IEC 27001:2013 en el componente de la Seguridad Física y del Entono, las organizaciones deben tener instaladas en las áreas de procesamiento de información alarma contra intrusos, contra incendios, y aplicar un sistema de seguridad física a las oficinas, salas e instalaciones de la organización, que realicen una acción preventiva frente a un suceso.

2- Conforme al Estándar COBIT en el objetivo de control Administración de las Instalaciones Protección contra Factores Ambientales, las organizaciones deben asegurar que se establezcan y mantengan las suficientes medidas para la protección contra factores ambientales como fuego, polvo, electricidad

Observaciones

1- El centro de datos no cuenta con un sistema de cámaras de seguridad.

2- Se evidencia que en el centro de datos no existe señalización que indique la prohibición de fumar y tomar alimentos en estos espacios, de igual forma en las áreas donde se encuentren alojados cualquier equipo de cómputo.

Riesgo

1- La Entidad se expone a:

- Acceso por personas no autorizadas al centro de datos.
- Daños de equipos de cómputo, electrónicos.
- Pérdida y/o robo de los equipos.

2- Se está expuesto a presentar daños en los equipos de cómputo, comunicaciones y servidores, con la consecuente pérdida de información y los costos de reparación que ello implica, en el evento de que éstos se vean afectados de presentarse un incendio o un daño por derrame de líquidos o alimentos.

Oportunidad de mejora

1- Es prudente que la Entidad analice el adquirir un sistema de vídeo vigilancia (cámaras de seguridad) y sistema de alarma contra incendios e intrusos, de tal forma que los equipos del centro de datos y la infraestructura estén protegidos.

2- Se sugiere instalar en el centro de datos de la Organización, señalización preventiva que prohíba fumar, tomar alimentos y bebidas en este espacio.

F. CONTROL DE ACCESOS

Sustento conceptual

1- De acuerdo a la Norma Técnica ISO IEC 27001:2013 en el objetivo de Políticas de Acceso a las Redes donde se garantiza la implementación y las medidas de seguridad para evitar amenazas, se deben llevar a cabo controles técnicos, que evalúen permanentemente los servicios de la red.

2- De acuerdo con la norma técnica ISO 27001:2013 en su objetivo de control 9.2.1 Gestión de altas/bajas en el registro de usuarios: Debería existir un procedimiento formal de alta y baja de usuarios con objeto de habilitar la asignación de derechos de acceso.

3- De acuerdo con los lineamientos de la Norma Técnica ISO IEC 27001:2013 en el objetivo de Seguridad de los Equipos en el ítem de políticas de puesto de trabajo despejado y de limpieza, donde se debe garantizar que al levantarse del puesto de trabajo y al finalizar la jornada laboral, los escritorios deben permanecer despejados y libres de documentos físicos y/o medios extraíbles que contengan información pública clasificada o pública reservada.

Observaciones

1- Se evidencia que no se cuenta con políticas, procedimientos y control de accesos a la red.

2- Se evidencia que no se lleva un control formal en el área de sistemas en el registro y baja de accesos (funcionarios).

3- No se cuenta con políticas de limpieza en el puesto de trabajo.

Riesgo

1- Se expone a:

- Pérdida de información por el acceso de personas no autorizadas a la red.
- Ataques mal intencionados en la red.

2- La Institución se expone a:

- Pérdida de información sensible.
- Vulnerabilidad de la información.
- Acceso a información sensible por parte de personal no autorizado.

3- Pérdida de información de los dispositivos extraíbles y/o equipos de computo por acceso no autorizado.

Oportunidad de mejora

1- Se sugiere establecer una política de accesos a los servicios de red, en la que es necesario especificar los derechos de acceso a cada red y los medios autorizados para dicho acceso, además de definir los procedimientos adecuados para obtener la autorización de derechos de acceso y los controles implantados para protegerse sobre el acceso no autorizado.

2- Es importante establecer una política de control de acceso a la gestión de usuarios para realizar los procedimientos formales de baja de accesos a los funcionarios y/o clientes, en caso que ya no hagan parte de la Entidad.

3- Se recomienda establecer políticas de limpiezas de puesto de trabajo y pantalla limpia para prevenir el acceso no autorizado, pérdida y/o daño de la información, equipos de cómputo, medios extraíbles, dispositivos de impresión y los puestos de trabajo deben permanecer limpios y ordenados.

G. ADMINISTRACIÓN DE INCIDENTES

Sustento conceptual

1- De acuerdo a los lineamientos de la Norma Técnica ISO IEC 27001:2013 en el objetivo de Gestión de Incidentes en la Seguridad de la Información, se debe garantizar las herramientas que le permitan actuar antes las posibles amenazas o debilidades que puedan poner en peligro la información sensible de la Empresa.

Observaciones

1- No se cuenta con una gestión de incidentes de la seguridad de la información y funcionamiento de los servicios.

Riesgo

1- Se puede presentar:

- Vulnerabilidad de la información.
- Pérdida de la información sensible de la Empresa.

Oportunidad de mejora

1- El primer objetivo de la gestión de incidentes es recuperar el nivel habitual de funcionamiento del servicio y minimizar en todo lo posible el impacto negativo en la Organización de forma que la calidad del servicio y la disponibilidad se mantengan.

H. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Sustento conceptual

1- Conforme a lo indicado en el Estándar Internacional COBIT, en el objetivo de control Aseguramiento del Servicio, la continuidad del negocio es el plan que crea una organización para restaurar sus funciones más importantes, interrumpidas total o parcialmente por algún incidente o desastre, dando respuesta en un tiempo determinado, por esto es importante diseñar un plan para la continuidad como medida de prevención para proteger los procesos críticos y operativos de la empresa, en este se incluyen los servicios telefónicos, información crítica, equipos, Internet, servidores entre otros.

Observaciones

1- Se evidencia que no hay documentación, ni implementacion de planes de contingencia y continuidad del negocio.

Riesgo

1- Se puede presentar:

- Pérdida de información irrecuperable y vital para la Organización.
- No tener identificados los diferentes eventos que pueden impactar las operaciones y su influencia en el negocio.
- No conocer los tiempos críticos de recuperación para volver a un estado normal de operación.
- Sufrir incidentes y no tener un plan logístico de respuesta rápida, Incurrir en gastos o pérdidas económicas en caso de ocurrir un incidente.

Oportunidad de mejora

1- Se sugiere implementar procesos de plan de contingencias y continuidad del negocio, realizando periódicamente simulacros o pruebas, con el fin de comprobar su efectividad.

B. RED DE DATOS

Actividad realizada

1 - La Entidad usa cableado estructurado de Categoría 6; próximamente en la nueve sede tendrán su cableado más actualizado y certificado.

2 - La Entidad esta pronto a trasladarse de sede, por lo que su proyección de ampliación de red esta casi lista.

Sustento conceptual

1- De acuerdo a la Norma Internacional ISO IEC 27001:2013 en el control de Seguridad en las Telecomunicaciones en el ítem políticas y control de red, las organizaciones deben contar con políticas aprobadas en cuanto al uso y seguridad de la red de datos.

2- De acuerdo a la Norma Internacional ISO IEC 27001:2013 en el control de Seguridad de los Equipos y Cableado, se deben garantizar que se encuentren óptimas condiciones del centro de datos.

3- De acuerdo a la Norma Internacional ISO IEC 27001:2013 en el control de Seguridad de los Equipos, en el ítem de instalaciones de suministro se deben garantizar que se encuentren óptimas condiciones del centro de datos.

Observaciones

1- No cuenta con políticas en cuanto al uso y seguridad en la red de datos.

2- Se evidencia que no hay Patch Panel en el centro de datos, están colocados en un escritorio con todo los cables, puesto que están próximos a trasladarse de sede.

3- Se puede observar que las canaletas en el centro de datos algunas se encuentran descubiertas y las paredes están deterioradas, rajadas y con mucha humedad.

Riesgo

1- La Organización está expuesta a problemas o fallos de conectividad, pérdida de información sensible, falta de conocimiento de los funcionarios.

2- La Empresa se expone a no garantizar el funcionamiento del centro de datos.

3- La Entidad se expone a no garantizar el funcionamiento correcto del centro de datos.

Oportunidad de mejora

1- Se recomienda crear, aprobar e implementar un documento de políticas de seguridad en la red de datos para prevenir fallos de conectividad.

2- Se recomienda realizar una reubicación del Patch Panel con su cableado bien organizado manteniéndolo limpio.

3- Se sugiere realizar una impermeabilización y arreglo de resanado a las paredes del centro de datos, instalando en los tramos de la red de datos nuevas tomas y canaletas, para optimizar el funcionamiento de los sistemas de información.

C. INTERNET

Actividad realizada

1 - La Cámara posee una conexión actual a Internet con la Empresa DIALNET con velocidad de 50 Megas, canal dedicado.

2 - La Entidad cuenta con un aplicativo contable, presupuesto, compras: JSP7 desarrollado por una Empresa proveedora llamada ASP Solutions S.A.

D. PROCEDIMIENTOS DE RESPALDO

Actividad realizada

1 - El aplicativo del Sistema de Registro Público administrado por CONFECAMARAS es responsable en la realización de backup y/o copias de respaldo.

Sustento conceptual

1- Conforme a lo indicado en el Estándar Internacional ISO IEC-27001:2013, en el control de Respaldo de la Información, hoy en día las organizaciones deben contar con procedimientos de respaldo de información, copias o backups, debidamente documentados, estableciendo su periodicidad y actividades complementarias.

2- Conforme a lo indicado en el Estándar Internacional ISO IEC-27002:2013, en el control Seguridad Operativa en el ítem de Registro y Eventos de Actividad de la Información define: hoy en día las organizaciones deben establecer una programación de sus procedimientos de respaldo y se cumplan según lo pactado.

Observaciones

1- Se observa que la Entidad no cuenta con un plan de backup, solo se realiza cuando se requiere algo sobre la máquina o algún mantenimiento que amerite; no tienen documentos de registros de las copias de respaldo, ni programación definida.

2- Se observa que las copias de respaldo (backups) de la información de usuarios no tiene una programación definida, es decir a consideración del usuario.

Riesgo

1- Pérdida de información sensible de la Entidad.

2- La Entidad está expuesta a pérdida de información irrecuperable.

Oportunidad de mejora

1- Es prudente considerar la realización de copias de respaldo de información de todos los sistemas de la Empresa diariamente, registrando en bitácoras las copias realizadas. Configurar controles de acceso de tipo encripción o claves en el disco externo extraíble donde se almacenan las copias de seguridad.

2- Se recomienda establecer una programación definida con el fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios del usuario.

F. ANTIVIRUS

Actividad realizada

1 - La Cámara cuenta con un software antivirus llamado SOPHOS, con una cobertura total.

G. CONTRATOS

Actividad realizada

1 - Actualmente la Entidad cuenta con los siguientes contratos suscritos:

- Para el servicio de Internet con el proveedor DIALNET.
- Arrendamientos de equipos con el proveedor PC COM S.A.
- Revision de Escaner e impresoras con el proveedor DATECSA S.A.
- Soporte del software DOCFLOW que es el sistema de gestión documental con el proveedor MAKROSOFT LTDA.
- Desarrollo de Sistema Contable del software JSP7 con el Proveedor ASP SOLUTIONS S.A.

Los cuales se encuentran actualizados, renovados, y contienen cláusulas de confidencialidad de la información.

H. PROYECTOS INFORMÁTICOS

Actividad realizada

1 - La Entidad cuenta con una persona encargada del área de desarrollo tecnológico de los proyectos informáticos, que es el Coordinador de Desarrollo e Innovación el cual lidera proyectos propios de la Entidad.

Sustento conceptual

1- Conforme con lo indicado en el Estándar Internacional COBIT, en el objetivo de control de administración de proyectos. Las organizaciones deben realizar una identificación, priorización, planeación y cronograma de actividades de los proyectos en línea con el plan de la empresa.

2- De acuerdo con lo indicado en el Estándar Internacional ISO IEC-27001:2013, en el control Seguridad en los Procesos de desarrollo y soporte, las organizaciones deben garantizar una metodología definida para cada proyecto informático a desarrollar, para el cumplimento y satisfacción de las necesidades del cliente.

Observaciones

1- Se evidencia que la Entidad no cuenta con un cronograma de actividades detallado para el cumplimiento de proyectos informáticos, recursos técnicos, financieros y humanos.

2- No se cuenta con una metodología para la ejecución de los proyectos informáticos.

Riesgo

1- Incumplimiento parcial o total de la ejecución en las metas y objetivos programados.

2- Incumplimiento en toda la ejecución del proyecto.

Oportunidad de mejora

1- Se recomienda nuevamente realizar un cronograma donde detalle los recursos, tiempo, actividades para cada uno de los proyectos por ejecutar en el departamento de sistemas.

2- Se sugiere implementar una metodología detallada de los proyectos a desarrollar, para no incurrir en entregas fuera del tiempo pronosticado y gastos adicionales de recursos de tiempo y humano, etc.

J. COMUNICACIÓN DE ÁREA CON LAS OTRAS ÁREAS

Sustento conceptual

1- De acuerdo a la Norma Internacional ISO IEC 27001:2013 en el control de organización de la seguridad de la información, las organizaciones deben definir de forma clara todas las responsabilidades y contar en sus áreas con el personal suficiente para atender los requerimientos, necesidades de los usuarios internos y externos.

Observaciones

1- Se puede observar que solo una persona es la encargada del área de desarrollo tecnológico, además de liderar además de parte estratégica, proyectos propios y planes de mejoramiento en la Entidad.

Riesgo

1- Incumplimiento en la atención de los requerimientos en materia de infraestructura tecnológica y desarrollo de proyectos informáticos.

Oportunidad de mejora

1- Se recomienda contar con el personal suficiente y asignar según sus roles y responsabilidades, para atender los diferentes requerimientos en el área de sistemas.

K. MANTENIMIENTO Y ASEO DE EQUIPOS

Sustento conceptual

1- Conforme a la Norma Técnica ISO IEC 27001:2013 en el objetivo de Seguridad de los Equipos se deben tener indicadores que muestren la eficiencia y eficacia de los equipos, para tomar decisiones sobre la evolución del mantenimiento.

Observaciones

1- No se cuenta con indicadores de gestión en los mantenimientos preventivos para medir su eficacia.

Riesgo

1- La Empresa se expone a:

- No garantizar el funcionamiento óptimo de la central de datos.
- Falta de análisis de reducción de costos.

Oportunidad de mejora

1- Se recomienda crear indicadores de gestión que demuestren la eficacia del mantenimiento preventivo con respecto al correctivo, para poder determinar la función óptima de los mantenimientos, ver el comportamiento operacional de las instalaciones, sistemas, equipos, medir la calidad de los trabajos y el grado de cumplimiento.