MUNICIPALIDAD DE ACOSTA
AUDITORÍA INTERNA MUNICIPAL
"Todos somos iguales ante el deber moral"

Acosta, 13 setiembre de 2022
Advertencia UAI-MA-007-2022

ADVERTENCIA

Señores (as)
Concejo Municipal

Norman Hidalgo Gamboa
Alcalde Municipal

MUNICIPALIDAD DE ACOSTA

Cordial saludo:

ADVERTENCIA: Sobre la revisión instrumento aplicación de prácticas de seguridad de la información en las instituciones públicas remitido por la Contraloría General de la República.

El servicio preventivo se realiza en uso de las competencias que le confiere el artículo 22 de la Ley General de Control Interno a la Auditoría Interna, cuyo inciso d), indica: *"Asesorar, en materiade su competencia, al jerarca del cual depende; además, advertir a los órganos pasivos que fiscaliza sobre las posibles consecuencias de determinadas conductas o decisiones, cuando sean de su conocimiento"*; conforme la Norma 1.1.4 y otros atributos definidos en las Normas para elEjercicio de la Auditoría Interna en el Sector Público; y de conformidad con la Norma 205 *Comunicación de resultados*, inciso 02, de las Normas Generales de Auditoría para el Sector Público.

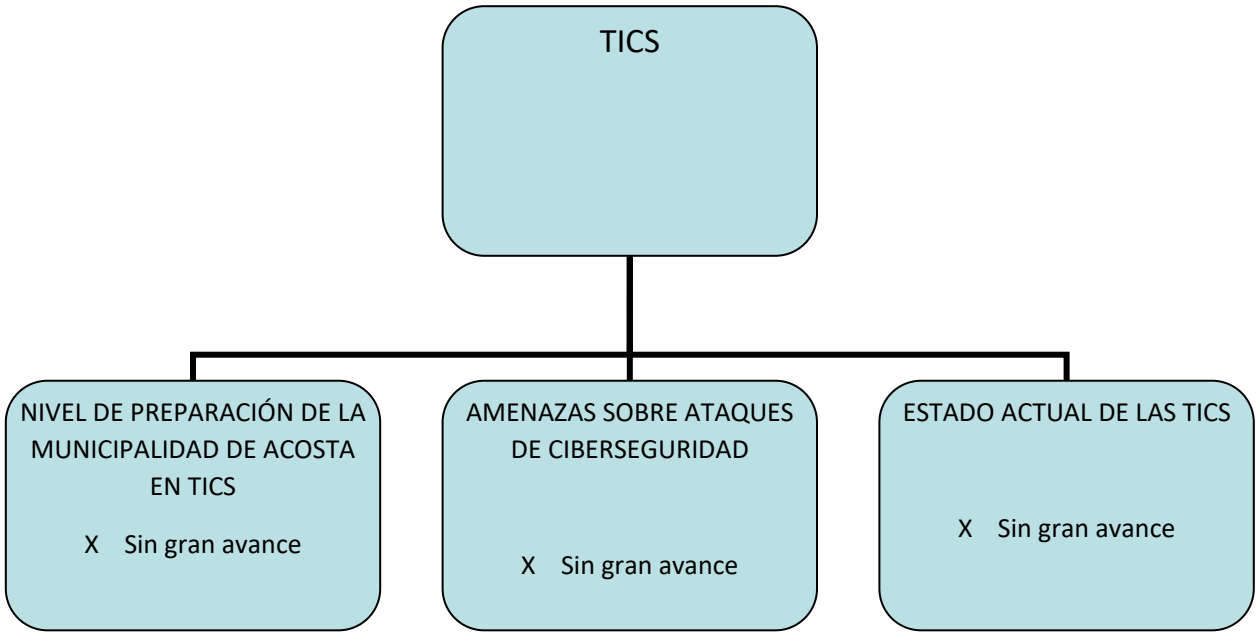
SITUACIÒN ENCONTRADA

En apego a las potestades de la Auditoría Interna estipuladas en el artículo 33 de la Ley General de Control Interno, con el fin de cumplir con lo estipulado en materia de responsabilidades asociadas a dicho ente fiscalizador respecto al Sistema de Control Interno de la Municipalidad de Acosta, se hace de conocimiento lo siguiente:

Con base al instrumento aplicación de prácticas de seguridad de la información en las instituciones públicas remitido por la Contraloría General de la República a la Administración Activa de esta Municipalidad y, de acuerdo a la revisión realizada de dicha

herramienta se logra determinar, que este Gobierno Local en la mayoría de los ítems formulados no cumple satisfactoriamente con los insumos a que se hace referencia, por lo que se podría determinar que el ayuntamiento se encuentra en un estado deficiente en cuanto a lo que manifiesta dicho documento.

A continuación, se muestra en resumen los resultados de la aplicación del instrumento de cara a la situación de esta municipalidad.



Con lo evidenciado, la Municipalidad de Acosta, podríamos casi tener una probabilidad razonable de que los riesgos de esta naturaleza se materialicen, por ausencia de mecanismos que vengan a mitigar estos eventos, por lo que el impacto que se generen de estos, serian catastróficos, hasta pudiendo generar la paralización del negocio en marcha.

A continuación, se muestra una tabla de probabilidades y de impacto, donde se estimaría la probabilidad de que la amenaza se materialice y el impacto sobre el negocio que esto produciría

Tabla para el cálculo de la probabilidad

Cualitativo	Cuantitativo	Descripción
Baja	1	La amenaza se materializa a lo sumo una vez cada año.
Media	2	La amenaza se materializa a lo sumo una vez cada mes.
Alta	3	La amenaza se materializa a lo sumo una vez cada semana.

Tabla para el cálculo del impacto

Cualitativo	Cuantitativo	Descripción
Bajo	1	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
Medio	2	El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la organización.
Alto	3	El daño derivado de la materialización de la amenaza tiene consecuencias graves reseñables para la organización.

Fuente: *Publicado el 16/01/2017, por INCIBE*

		IMPACTO		
		Bajo	Medio	Alto
PROBABILIDAD	Baja	Muy bajo	Bajo	Medio
	Media	Bajo	Medio	Alto
	Alta	Medio	Alto	Muy alto

Fuente: *Publicado el 16/01/2017, por INCIBE*

Según lo descrito, como se puede apreciar al estar ayuna la Municipalidad de casi todos los insumos requeridos para la buena marcha del negocio en cuanto a las Tecnologías de Información y Seguridad (TICS), se corre el peligro de que el riesgo podría materializarse en cualquier momento y el daño derivado de la materialización de la amenaza conlleve a consecuencias graves reseñables para este Gobierno Local.

Se describe a continuación la situación encontrada con respecto a dicha herramienta.

DIMENSIÓN 1: ESTRATEGIA Y ESTRUCTURA

Comprende la evaluación de las acciones ejecutadas por el jerarca para el establecimiento de la ruta a seguir tanto a nivel estratégico como operativo, en procura de un desempeño eficiente y eficaz de la aplicación del sistema de gestión de la seguridad de la información y ciberseguridad institucional.

A. ESTRATEGIA Y MECANISMOS DE CONTROL

1.1. No se dispone de un Sistema de Gestión de la seguridad de la información.

1.2. La institución no dispone de procedimientos y/o políticas de seguridad de la información, no tiene establecidas directrices sobre la seguridad de la información, asimismo no involucran el manejo de la Ciberseguridad entendida como el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberespacio.

Por lo tanto, hay ausencia de i- Mecanismos para asegurar una protección razonable de los activos tecnológicos y la información, ii- Clasificación de activos tecnológicos e información según confidencialidad, integridad y disponibilidad, iii- Elementos que propicien un ambiente seguro considerando la seguridad física y ambiental, iv- Mecanismos para prevenir, detectar, impedir, valorar, evaluar y corregir vulnerabilidades en la seguridad, v- Controles para proteger la confidencialidad, autenticidad, privacidad e integridad de la información, vi- Plan de capacitación, formación y actualización para el personal encargado en seguridad de la información y seguridad, vii- Mecanismos para gestionar las contrataciones de servicios con terceros, viii- Mecanismos sancionatorios ante incumplimiento del procedimiento y/o políticas, ix- Mecanismos para dar seguimiento a la implementación de los procedimientos y/o políticas.

Se menciona que a pesar no contar con documentación escrita, se cuenta con firewall en condición de préstamo por parte del IFAM.

1.3 La institución no tiene implementados lineamientos sobre los roles y responsabilidades para el personal encargado de la protección de la información y sistemas de información, del acceso, uso, divulgación, alteración, modificación o destrucción no autorizada, con el fin de garantizar la

confidencialidad, integridad y disponibilidad. Así como de la Ciberseguridad, entendida como el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberespacio.

Se hace la salvedad, que el Departamento de Informática el responsable es un funcionario, cuya plaza es de medio tiempo.

1.4 La Municipalidad no ha formalizado: Planes de continuidad de negocio para los servicios críticos de la institución, basados en los análisis de impacto al negocio, Planes, procesos y procedimientos para el manejo de incidentes de seguridad y ciberseguridad (planes de respuesta), Planes de recuperación de incidentes, Sitios alternos de procesamiento, de acuerdo al análisis de impacto del negocio.

Se hace la anotación que la institución cuenta con un Plan de Contingencia

B. GESTIÓN DE RIESGOS

1.5 Se menciona que, si se cuenta e implementa una gestión de riesgos, pero no incorpora la seguridad de la información, se hace de conocimiento que no existe un documento como tal, pero si se realizan los procesos de respaldos periódicos de información sensible.

Por lo tanto al no tener documentado la gestión de riesgos de seguridad de la información no se consideran los siguientes puntos: i- El marco normativo en que se basa la gestión de riesgos sobre la seguridad de la información, ii- El análisis de los riesgos y su impacto en la institución, iii- Medidas para la administración de los riesgos, iv- El monitoreo de los riesgos relevantes para el logro de los objetivos asociados a la seguridad de la información, v- Asignación de los recursos para las acciones de mitigación de riesgos, vi- Los roles y responsabilidades de los encargados de la gestión de riesgos, vii- La tolerancia-límite de riesgo aceptable de la institución.

1.6 La institución no cuenta con una matriz de riesgo de todos los activos relacionados con la información crítica o sensible.

1.7 No se disponen de mecanismos para la identificación de desviaciones conforme a la tolerancia-límite de riesgo definido como aceptable.

1.8 No se han efectuado estudios de impacto sobre el funcionamiento de la entidad, en caso de materializarse riesgos relacionados con la pérdida de activos de información.

B. SEGUIMIENTO Y CONTROL

1.9 En la institución se efectuó una auditoría en el 2018 para medir la efectividad del Sistema de Gestión de seguridad de la información, del cual la Auditoría Interna giro recomendaciones, pero a la fecha se podría decir, que hay incumplimientos de las mismas, a continuación, se detallan las recomendaciones realizadas:

Al Sr. Alcalde Municipal

a. En coordinación con el ejecutor del proceso Tecnología de Información, supervisar el cumplimiento de los siguientes procesos de las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE) de la Contraloría General de la República de Costa Rica:

1.1 Marco estratégico de TI
1.3 Gestión de riesgos
1.4 Gestión de la seguridad
1.4.7 Continuidad de los servicios (plan de contingencias)
1.6 Decisiones sobre asuntos estratégicos de TI
2.1 Planificación de las tecnologías de información
2.4 Independencia y recurso humano de la Función de TI

b. El Alcalde es el responsable del control interno y el cumplimiento de la normativa de TI de la Contraloría General de la República de Costa Rica.

c. Asignar al personal administrativo la observación de este estudio, verificar que existan fechas específicas para cumplir con las observaciones y supervisar la realización de las recomendaciones del estudio:

i. 2.1 inciso a: Ausencia un marco estratégico de TI

ii. 2.1 inciso b: Ausencia de un plan estratégico de TI

iii. 2.2 inciso a: Ausencia de un proceso de gestión de riesgos

iv. 2.2 inciso b: Revisión de licencias de software
v. 2.3 inciso a: No se ha implementado un marco de seguridad de la información
vi. 2.3 inciso b: No existe un proceso para garantizar la seguridad del sistema
vii. 2.3 inciso c: Ausencia de administración de la seguridad de TI
viii. 2.3 inciso d: Ausencia de un plan de seguridad de TI
ix. 2.4 inciso a: Ausencia de políticas o información sobre la seguridad de la información
x. 2.5 inciso a: No existe un proceso para seguridad física y ambiental
xi. 2.5 inciso b: Existen debilidades en el cuarto de servidores
xii. 2.6 inciso a: Ausencia de seguridad de TI en las operaciones y comunicaciones
xiii. 2.6 inciso b: Falta un antivirus
xiv. 2.6 inciso c: Falta un Firewall y un Sistema de detección de intrusos
xv. 2.7 inciso a: Ausencia de proceso de seguridad en la implementación y mantenimiento de software e infraestructura tecnológica
xvi. 2.8 inciso a: No existe un proceso de continuidad de los servicios de TI
xvii. 2.8 inciso b: Ausencia del proceso de garantizar la continuidad del servicio
xviii. 2.8 inciso c: Ausencia de planes de Continuidad de TI
xix. 2.8 inciso d: No existen respaldos fuera de la Municipalidad
xx. 2.8 inciso e: Ausencia de una política documentada de respaldos
xxi. 2.8 inciso f: Ausencia de política y procedimientos de recuperación
xxii. 2.9 inciso a: Ausencia de un marco de Gestión de TI
xxiii. 2.10 inciso a: No existe un proceso de planificación de las tecnologías de información
xxiv. 2.10 inciso b: Ausencia de un plan de adquisición de sistema contable
xxv. 2.10 inciso c: Ausencia un plan de adquisición de un sistema presupuestario
xxvi. 2.11 inciso a: Ausencia de un proceso para la Infraestructura tecnológica
xxvii. 2.11 inciso b: Ausencia de planificación de la Dirección Tecnológica
xxviii. 2.11 inciso c: Ausencia de plan de Infraestructura Tecnológica
xxix. 2.12 inciso a: a. Ausencia en la definición de los Procesos, Organización y Relaciones de TI
xxx. 2.12 inciso b: La Estructura Organizacional de TI debe ser analizada
xxxi. 2.12 inciso c: Falta segregación de funciones en TI
xxxii. 2.12 inciso d: Análisis de las habilidades y competencias del personal de TI
xxxiii. 2.12 inciso e: Existe dependencia en el encargado de TI

Esta recomendación se dará por atendida con el envío de parte del alcalde a la Auditoría Interna del oficio donde hace constar la implementación de las medidas correctivas correspondientes en el plazo que no sobrepase el 20 de diciembre de 2018.

4.2 Al Sr. Encargado de TI

Realizar las actividades asignadas por el Alcalde de los procesos de las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE) de la Contraloría General de la República de Costa Rica en que existe incumplimiento.

Esta recomendación se dará por atendida con el envío de parte del encargado de TI a la Auditoría Interna del oficio donde hace constar la implementación de las medidas correctivas correspondientes en el plazo que no sobrepase el 20 de diciembre de 2018.

1.10 Con respecto al marco normativo y protocolos establecidos por la entidad rectora en seguridad de la información y ciberseguridad (MICITT).

Según anotaciones se indica que se conoce y se aplica el marco normativo y sus protocolos, a la vez se menciona que la Municipalidad aplicará la herramienta facilitada por el MICITT, para el marco estratégico, sin embargo la falta de tiempo y capacitación del personal no han permitido avanzar en este tema, sin embargo se están haciendo esfuerzos para contratar una empresa que nos colabore.

DIMENSION 2: LIDERAZGO Y CULTURA:

En esta dimensión se contempla la evaluación de las acciones ejecutadas por el jerarca en cuanto a la definición e implementación de líneas rectoras y orientadoras para direccionar y guiar el sistema de gestión de seguridad de la información y ciberseguridad, en miras de lograr el resguardo de la información y continuidad del servicio.

A. GOBIERNO CORPORATIVO, CULTURA ORGANIZACIONAL Y SEGURIDAD DE LA INFORMACIÓN.

2.1 El jerarca contempla que la información es para la institución, con respecto a este ítem la pregunta quedó sin contestar, por lo que se presume que no hay un criterio respecto a la visión del máximo jerarca en cuanto a la percepción de la información institucional.

2.2 La institución visualiza la seguridad de la información como una inversión que anticipa riesgos y asegura la operación institucional.

Se indica que se ha presupuestado varias veces el tema de licenciamiento, antivirus y otros aspectos, sin embargo, por la situación financiera de la municipalidad no ha sido posible llevar a cabo las compras.

2.3 La institución no ha integrado la seguridad de la información a los distintos procesos institucionales. Se menciona que es un proceso separado de la gestión operativa institucional.

2.4 Se menciona que si se aplican mecanismos hacia el personal institucional con el fin de evaluar su percepción y conciencia de ciberseguridad, esto se realiza mediante envió de correos u oficios para tratar de concientizar a los usuarios internos (MA-DTI-15-2022 y MA-DTI-16-2022).

2.5 Al no existir un Código de ética o conducta, no se ha definido el comportamiento esperado del personal acerca de la recolección y manejo de la información sensible o critica.

B. CONCIENTIZACIÓN AL PERSONAL SOBRE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD.

2.6 Con respecto a la disposición de un programa de sobre la concientización vigente hacia el personal sobre la seguridad de la información acorde con los procedimientos y/o políticas de seguridad de la información, solo responde que se consideran los ítem a) y b).

a) La comunicación de la información institucional que debe protegerse y b) Los controles que se han establecido para proteger la información.

Resultando que para los ítems de la c) a la i) no cuenta con nada establecido.

DIMENSIÓN 3: PROCESOS E INFORMACIÓN

La dimensión considera aspectos que comprenden la evaluación del esquema formal definido para el desempeño del sistema de gestión de seguridad de la información y ciberseguridad institucional, así como la forma en la cual se asegura la obtención de información relevante para la toma de decisiones, con el fin de lograr el resguardo de la información y continuidad del servicio.

A. SEGURIDAD DE LA INFORMACIÓN: MANEJO Y CUSTODIA DE LA INFORMACIÓN

3.1 La institución no cuenta con certificaciones relacionadas con el Sistema de Gestión de seguridad de la información.

3.2 No se encuentran identificados los procesos críticos en la institución, se menciona que no aunque no existe un documento formal, si se conocen cuáles son los procesos críticos.

3.3 No se ha identificado y clasificado la información crítica y/o sensible de la institución.

3.4 Se menciona que se ha elaborado un inventario de más del 50% de los activos y dispositivos informáticos, asimismo no se categorizan los activos críticos y que la periodicidad con que se actualiza el inventario es una vez al año.

3.5 Se menciona que se realizan copias de seguridad de los sistemas críticos y sus respectivas bases de datos, una vez al día, aun así se indica que no existen documentos que respalden esas copias de seguridad.

3.6 No se realizan copias de los respaldos fuera de la institución, ejemplo centro de datos o en servicios en la nube.

3.7 Se señala que si se realizan pruebas de funcionalidad a los respaldos de información para valorar si permiten restaurar los servicios críticos, a la vez se indica que se realiza una vez al año, asimismo se menciona que no existe documento que respalde esto.

3.8 Se hace alusión que se encripta alguna información almacenada clasificada como crítica o sensible, mediante copias de seguridad en Windows server, igualmente no existe documento de respaldo.

3.9 No se cuentan con mecanismos para encriptar la información en tránsito.

3.10 No se cuenta con segmentación de la red.

3.11 No se cuenta con la implementación de los siguientes componentes: a- EDR, b- IDS-IPS, D-DMZ, se menciona que solo se cuenta con Firewalls, en condición de préstamo por parte del IFAM, el cual ya se encuentra operando, sin embargo, aún no han formalizado el convenio.

3.12 Se indica que no se realiza un monitoreo periódico de la red.

3.13 No se realiza un análisis periódico de la capacidad de servidores y dispositivos, con el fin de detectar un consumo excesivo de recursos que pueden identificar problemas de seguridad.

3.14 La Municipalidad no posee o implementado un plan para la gestión de los incidentes, que venga a minimizar los impactos negativos en las instituciones que reportan incidentes de soporte técnico y corregir los errores.

3.15 La Municipalidad no ha realizado simulacros o pruebas de manejo de incidentes durante los años 2021 y 2022.

3.16 No se cuenta con indicadores que midan el grado de seguridad obtenido de los resultados del simulacro o prueba de manejo de incidentes.

B. CIBERSEGURIDAD: APLICACIONES BÁSICAS EN LA INSTITUCIÓN

3.17 La Municipalidad cuenta con mecanismos de protección ante amenazas tales como: Firewalls (red, web, etc), Red Privada virtual (VPN), Filtradores de páginas web, todas estas acciones se dan gracias al Firewall prestado por el IFAM, asimismo se carece de Antivirus en los equipos, bloqueadores de scripts habilitados, Anti Ransomware, Servidores Proxy.

3.18 No se realizan pruebas de seguridad como Pentesting o Análisis Vulnerabilidades.

3.19 No se realiza un plan de acción a partir de los resultados del análisis de vulnerabilidades, considerando la priorización, calendarización y responsables para subsanar las debilidades resultantes de esos análisis.

DIMENSIÓN 4: COMPETENCIAS Y EQUIPOS

En esta dimensión se contemplan las acciones desarrolladas por el jerarca para la definición de las habilidades, conocimientos y aptitudes requeridas por el personal responsable del sistema de gestión de la seguridad de la información y

ciberseguridad, así como de las actividades implementadas para el resguardo de la información y la continuidad del servicio.

A. COMPETENCIAS DEL PERSONAL EN SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD.

4.1 La institución no ha definido y revisado los requisitos técnicos y de idoneidad del perfil del personal en seguridad de la información y ciberseguridad. Se hace mención que no se dispone de ese personal.

4.2 No se cuenta con un plan de capacitación institucional sobre temas de Ciberseguridad.

4.3 No se ha capacitado al personal sobre ciberseguridad periódica, encargado de la ciberseguridad de la información.

B. COLABORACIÓN Y TRANSFERENCIA DE CONOCIMIENTOS.

4.4 La Municipalidad no promueve el trabajo colaborativo entre los diferentes departamentos de la institución y el personal a cargo de los procesos de seguridad de la información y ciberseguridad, por lo que no realiza las siguientes acciones: a- Apoyar iniciativas e integración del personal con el fin de optimizar las acciones y toma de decisiones sobre temáticas en común, b- Impulsar actividades para el intercambio de aprendizajes entre las personas colaboradoras que laboran en entidades del sector público que sean afines, c- Desarrollar estrategias para abordar los factores que obstaculizan el trabajo colaborativo institucional, d- Se promueve el aprendizaje institucional en temas de seguridad de la información y ciberseguridad mediante la comunicación de buenas prácticas y lecciones aprendidas.

ELEMENTOS DE PRESUPUESTOS Y COMPRAS PÚBLICAS

A. PRESUPUESTO ASOCIADO A LA CIBERSEGURIDAD.

1- La Municipalidad no presupuestó para los años 2021 y 2022 gastos asociados a la ciberseguridad.

2- La Municipalidad no ha presupuestado recursos para la adquisición de bienes o servicios en relación al tema de seguridad de la información y ciberseguridad.

3- La Municipalidad no ha realizado proyecciones de necesidades de gastos adiciones a mediano plazo (aproximadamente 2 años) en temas de seguridad de la información o ciberseguridad.

B. COMPRAS PÚBLICAS ASOCIADAS A CIBERSEGURIDAD.

1- La Municipalidad no ha realizado ajuste en el presupuesto para compra asociadas a ciberseguridad.

2- La Municipalidad no ha realizado contrataciones asociadas a la emergencia nacional (ciberataques) con base en el artículo 40 bis de la Ley de Contratación Administrativa.

Se menciona que si se han detectado prácticas y/o aprendizajes, como es concientizar al usuario interno sobre el phishing, temas de cambio de contraseñas periódicas.

Se alude que, como aprendizaje institucional, la Municipalidad de Acosta está muy limitada con respecto a estos temas debido a la falta de presupuesto, capacitación y personal para desarrollar un espacio seguro y confiable como realmente lo deseamos, se dice que debería de existir más apoyo y acompañamiento por parte de diferentes instituciones públicas a instituciones pequeñas como la nuestra, donde se dificulta bastante cumplir con todos estos requerimientos.

ASPECTOS A CONSIDERAR.

A la luz de la información brindada por la Administración, mediante el llenado de la herramienta remitida por el ente de fiscalización superior (C.G.R.), se advierte lo siguiente:

1- El Departamento de Informática de la Municipalidad de Acosta, no cuenta con personal especializado en la materia, asimismo no cuenta con contenido presupuestario para contratar gestión de apoyo de un especialista para que coadyuve en la implantación de lo requerido según dicha herramienta, al mismo tiempo el encargado de informático es una plaza de medio tiempo.

2- A pesar de que el Plan Estratégico Institucional que va del 2019 al 2023, donde uno de sus objetivos está el fortalecimiento del Departamento de T.I. y

Comunicación, al día de hoy no se han realizado acciones para su cumplimiento, quedando ese objetivo solamente escrito en prosa.

3- El Jerarca Administrativo, como responsable del Sistema de Control Interno Institucional, según lo mencionan las Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE) en especial las Normas 1.1 (Sistema de Control Interno, 1.4 (Responsabilidad del Jerarca y los titulares subordinados sobre el SCI), Norma 5.8 (Control de Sistemas de Información) y la Norma 5.9 (Tecnologías de Información), debe velar razonablemente que se cumplan al menos lo siguiente:

3.1 Que asegure que los objetivos de seguridad informática estén establecidos, que cumplan los requisitos de la institución y estos se encuentren integrados en los procesos principales.

3.2 Que formule, revise y apruebe las políticas de seguridad informática.

3.3 Que las políticas de seguridad informática sean efectivas desde su implementación.

3.4 Debe brindar en las medidas de las posibilidades institucionales los recursos necesarios para la seguridad informática.

3.5 Que se asegure que la implementación de todos los controles de seguridad informática sea coordinada en toda la Municipalidad.

4- El Jerarca Institucional y el Encargado de Informática, deben valorar realizar una evaluación de riesgos, orientadas a determinar los sistemas que, en su conjunto o en cualquiera de sus partes, pueden verse afectados directa o indirectamente por amenazas, valorando los riesgos y estableciendo sus niveles a partir de las posibles amenazas, las vulnerabilidades existentes y el impacto que puedan causar a la institución.

5- Se debe valorar realizar una Gestión de Riesgos, que implique identificar, seleccionar, aprobar y manejo de los controles a establecer para eliminar o reducir los riesgos evaluados a niveles aceptables, con acciones como las siguientes:

a- Reducir la probabilidad de que una amenaza ocurra
b- Limitar el impacto de una amenaza, si esta se manifiesta
c- Reducir o eliminar una vulnerabilidad existente,
d- Permitir la recuperación del impacto o su transferencia a terceros.

Finalmente, se le exhorta a implementar las medidas correctivas y preventivas que correspondan de conformidad con el ordenamiento jurídico atinente, en atención a lo advertido por esta Auditoría.

Se solicita remitir en un **plazo de diez días**, posterior a la remisión del presente documento, el informe de las acciones y decisiones que se hayan dispuesto al respecto; con el fin de brindar elseguimiento que exige la normativa.

Cordialmente,

PEDRO MIGUEL JUAREZ GUTIERREZ (FIRMA)

Firmado digitalmente por PEDRO MIGUEL JUAREZ GUTIERREZ (FIRMA)
Fecha: 2022.09.13 11:25:22 -06'00'

Lic. Pedro M. Juárez Gutiérrez
Auditor Interno

Cc/archivo.