INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO

ESPECIALIZACIÓN SEGURIDAD DE LA INFORMACIÓN

MODELO POLÍTICAS EN SEGURIDAD DE LA INFORMACIÓN EN LA ALCALDIA DE PARATEBUENO

PRESENTA:

ANA MISSLEY BERMUDEZ BARRETO
CÓDIGO 1622010198

ASESOR TEMÁTICO:

WILMAR JAIMES FERNANDEZ

MARZO DEL 2018

VILLAVICENCIO

ÍNDICE GENERAL

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

Actualmente los sistemas informáticos están expuestos a un alto número de vulnerabilidades que constituyen un riesgo sobre el activo más crítico y vulnerable de las entidades como lo es la información.

Las entidades como objetivo fundamental tienen el velar por asegurar la disponibilidad, la confidencialidad y la preservación de datos, es un servicio de estricto cumplimiento, donde las políticas de seguridad juegan un papel importante, proceso que debe estar bien documentado y referido.

El desarrollo de este proyecto se refiere a un diseño metodológico para la construcción de los lineamientos en las políticas de seguridad informática en la Alcaldía del Municipio de Paratebueno Cundinamarca, las cuales garantizarán el nivel de seguridad y permitirán proteger el activo fundamental de la información.

La elaboración de estas políticas de seguridad en la alcaldía Municipal es una decisión de gran importancia y fundamento cuando se trata de proteger el activo más importante como lo es la información, es el objetivo esencial proteger dicho activo a través de controles, de buenas prácticas, lineamientos y reglas que deben ser aplicadas en la entidad dirigidas y apoyadas por el representante legal.

Palabras clave: Seguridad, Información, Confidencialidad, Integridad, Disponibilidad.

ABSTRACT

Currently, computer systems are exposed to a high number of vulnerabilities that constitute a risk to the most critical and vulnerable assets of entities, such as information.

Entities as a fundamental objective have to ensure the availability, confidentiality and preservation of data, is a strict compliance service, where security policies play an important role, a process that must be well documented and referred.

The development of this project refers to a methodological design for the development of computer security policies in the Municipality of Paratebueno Cundinamarca, which will guarantee the level of security and will protect the fundamental asset of information.

The development of this project refers to a methodological design for the construction of guidelines on computer security policies in the Municipality of Paratebueno Cundinamarca, which will guarantee the level of security and will protect the fundamental asset of information

Key words: Security, Information, Confidentiality, Integrity, Availability.

INTRODUCCIÓN

Este proyecto tiene como finalidad diseñar políticas de seguridad de la información para un ente territorial, donde se implementarán lineamientos confiables que en base de la política institucional proteja los activos de la Entidad.

La principal característica de las políticas de seguridad es asegurar el buen funcionamiento y facilitar los procesos para los empleados y usuarios de la Alcaldía del Municipio de Paratebueno, ofreciendo mejoras en sus módulos a nivel de seguridad, teniendo en cuenta que se maneja información de gran importancia a nivel público. Para analizar la problemática es necesario realizar un diagnóstico donde se identifique las falencias que presenta el sistema de seguridad informática de la entidad. Por consiguiente, dichas falencias se presentan por la ausencia de protocolos de seguridad, originando que los sistemas de información sean más vulnerables a perdida y alteración de la información.

De acuerdo al estado actual de la Alcaldía de Paratebueno, se debe evitar y prevenir que la información y el servicio se vea involucrado en incidentes de seguridad por falta de medidas mínimas como controles, responsabilidades y roles definidos y documentados conocidos e implementados por todos los funcionarios públicos del ente territorial.

Con estas políticas de seguridad el ente territorial podrá evaluar regularmente los diferentes procesos, los mecanismos para responder eficazmente ante los incidentes de seguridad y disminución de riesgos y ofrecerá a los empleados las herramientas necesarias para actuar con responsabilidad frente a su trabajo y labores ejecutadas a diario.

La aplicabilidad y el éxito de la política depende del diseño estricto a las necesidades de la entidad para el desempeño de sus logros en la mitigación de riesgos y amenazas y la

vinculación de todo el personal incluyendo la parte directiva que es fundamental para su implementación.

.

1. PLANTEAMIENTO DEL PROBLEMA

La alcaldía del Municipio de Paratebueno Cundinamarca como entidad pública está encargada de gobernar la acción administrativa del Municipio, ofreciendo a la comunidad trámites y servicios, cuenta con diferentes medidas las cuales permiten como objetivo principal de optimizar la Seguridad de la Información en la entidad, pero existen circunstancias al interior que retrasan los procesos, como lo es no contar con un sistema de información que mitigue los riesgos, de igual manera la falta de concientización de parte de los empleados públicos en cuanto a seguridad, donde no es considerado algún tipo de información de importancia para la entidad.

La alcaldía no posee un método de información apropiado, lo que no admite establecer el estado actual en seguridad del ente territorial, la información de los servidores públicos, los debidos procesos y la tecnología, por lo tanto, no se tiene implementado una planeación y caracterización de revisiones de seguridad fundamentados en la estimación de alarmas y su respectiva medición.

Es por este que nace la necesidad de diseñar una metodología para la implementación de políticas de seguridad, que permita proteger y conservar la información en la entidad pública. Las políticas de seguridad deben ser de carácter obligatorio para todos los empleados públicos y personas externas que necesiten de la información de la Administración Municipal, de igual forma a todas las dependencias que hacen parte de los componentes de seguridad de información, de manera argumentada, metódica, eficaz y acondicionada en cambios originados en los riesgos, el medio y los procesos de la información.

En la entidad Municipal se identifican algunas problemáticas con los Sistemas de información, como son los ingresos a centros de cómputo no autorizados, la falta de

actualización de aplicativos en todos los dispositivos de computación de la entidad, y la falta de control en el uso de usuarios y contraseñas de los diferentes equipos. La carencia de políticas de seguridad y el manejo inadecuado de los usuarios en una entidad pública que fortalece los procesos de desarrollo del Municipio, puede constituir causales de perjuicios al sector público del País.

2. FORMULACION DEL PROBLEMA

¿Cómo Diseñar el Manual en políticas en seguridad de la información para la Alcaldía Municipal de Paratebueno?

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar el modelo de políticas y lineamientos con el fin de mitigar las amenazas y vulnerabilidades en la Alcaldía Municipal de Paratebueno.

3.2 OBJETIVOS ESPECÍFICOS

- Hacer un análisis de riesgos y vulnerabilidades existentes, con el fin de ofrecer una perspectiva a nivel general de las vulnerabilidades en las dependencias y secretarias de la Alcaldía de Paratebueno y así determinar la situación actual del ente territorial.
- Analizar los resultados obtenidos identificando las causas, falencias y sitios vulnerables de la entidad.

4 JUSTIFICACIÓN

Actualmente la Alcaldía Municipal de Paratebueno, presenta gran número de falencias de seguridad informática en las dependencias del ente territorial, por lo cual se hace necesario realizar un análisis de las diferentes vulnerabilidades que se presenta con la

protección en datos y los diferentes lineamientos en la entidad en busca de garantizar la seguridad en la información.

De acuerdo a esto surge la necesidad diseñar un modelo de políticas en seguridad informática para brindar solución a los diferentes incidentes que se exteriorizan en la Alcaldía Municipal de Paratebueno, adoptando mecanismos y controles que ayuden a mitigar impactos de la seguridad de la información, ya que estos pueden ser puntos críticos para la ejecución de las actividades en la entidad territorial.

5 ALCANCE

Este proyecto está enfocado a tener presente el diagnostico a través del levantamiento y estudio de la seguridad informática de la Alcaldía Municipal de Paratebueno Cundinamarca ubicada en la Kra 9 No 3-30 Centro, referente a la problemática de delito informático, perdida de información, ataques cibernéticos, teniendo presente los elementos que contribuyan con criterios que permitan realizar correcciones importantes y significativas de acuerdo a la importancia de las auditorias informáticas con la finalidad de disminuir y controlar las amenazas de los sistemas de información en el ente territorial.

6. MARCO INVESTIGATIVO

6.1 TIPO DE INVESTIGACION

De acuerdo a las características del proyecto y la lógica del entregable, el marco referencial lo establece la investigación técnica apropiada.

6.2 METODOLOGIA

Para este proyecto el tipo de investigación con la cual se va desarrollar este proceso es el cuantitativo, teniendo en cuenta que de esta manera se puede obtener el conocimiento y elegir

un modelo adecuado que permita conocer la realidad del objeto de estudio y poder analizar los datos recolectados por medio de los conceptos y las variables que se manejen.

La metodología que se va a llevar a cabo está basada en las normas ISO/IEC 27001, de acuerdo a las necesidades de la Alcaldía Municipal de Paratebueno. Esta metodología estará implementada con los objetivos planteados en el proyecto para su ejecución.

En primer lugar, se realizará un levantamiento de la información de las experiencias de seguridad y del estado actual de la información en la entidad. La finalidad de este proceso, permitirá entregar el insumo base para poder realizar el análisis de las políticas a implementar en el interior de la entidad territorial.

En segundo lugar, con el trabajo elaborado se establecerán los requisitos para la elaboración de las políticas apropiadas que convengan para garantizar la seguridad en la información.

Finalmente se dará a conocer a los servidores públicos y Secretarios de despacho, representante legal de la Alcaldía Municipal, las reglas y normas adecuadas en el uso de los sistemas de información que están dispuestos para realizar las actividades laborales diarias, y de esta manera minimizar el riesgo de pérdida, daño y alteración de la información, de igual forma para tener conocimiento de cómo actuar al momento de una violación de seguridad, provenientes de sujetos internos o externos.

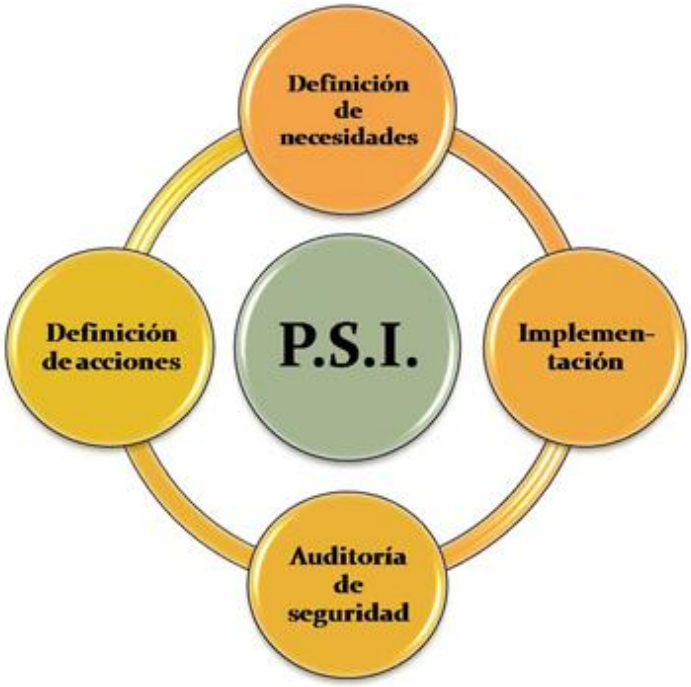

Figura 1. Política de seguridad informática

7. FUNDAMENTACION TEORICA

7.1 MARCO HISTÓRICO

7.1.1 SEGURIDAD INFORMATICA

Con el avance del internet y su uso universal en las empresas la Seguridad a nivel de información se encamino hacia la conexión haciendo uso de las redes, resguardando los ordenadores de software informáticos, y los ordenadores asequibles oficialmente con el uso del internet, realizando control de la seguridad a nivel periférico utilizando mecanismos como lo es el corta fuegos.

La figura del atacante de un sistema de información ha ido cambiando con la evolución de la tecnología. Anteriormente los objetivos de un atacante se consideraban más sencillos, actualmente los atacantes han resaltado de la importancia de la información y del valor para las entidades de esta. Estos atacantes están conformados en organizaciones, los cuales aprovechando las falencias y debilidades de los sistemas de información y de las redes tele

comunicativas con el fin de tener acceso a la información privada y confidencial de la entidad, ya sea por intermedio de personas expertas en realizar estos ataques, o de igual forma con la compra de paquetes ilegales para detectar las vulnerabilidades y facilitar el acceso a la información detalla y privada en la empresa.

Las nuevas modalidades para realizar ataques informáticos, los cambios en la figura de los agresores, e igualmente la importancia vital de la información privada y confidencial para el desempeño de las entidades, contribuyen para evolucionar del tema de la seguridad informática al significado real de la seguridad en la información, donde el objetivo primordial reside en organizar las transformaciones de la seguridad frente al objetivo general de la entidad y tácticas para el desarrollo de las actividades empresariales. Cuando se habla de seguridad de la información se hace referencia al plan de Políticas de Seguridad constituida en los procedimientos estratégicos de la entidad. Para definir estas políticas es de vital importancia contar con todos los factores, como lo es la ubicación de la entidad, dimensión, sedes, condición geográfica, cumplimiento de la ley y normas vigentes.

Es imperioso para la entidad tener conocimiento continuamente del valor de su activo más decisivo y precioso, como lo es la información de la entidad, conocer las brechas falencias de seguridad las cuales facilitarían al acceso a la información. De igual manera nace la necesidad de estar informado del estado en seguridad de manera permanente mediante la realización del análisis de riesgos los cuales otorguen la identificación de las primordiales amenazas y medir los riesgos incorporados con la ejecución de estas, finalmente hay que tener en cuenta diferentes componentes importantes, como lo es el valor de la información, la posibilidad de que una amenaza se presentara, y por último el impacto que ocasionaría sobre la entidad la ejecución de dicha amenaza.

7.2 MARCO TEÓRICO

7.2.1 SEGURIDAD INFORMATICA

Actualmente, todas las entidades utilizan la información como una herramienta básica para la toma decisiones, siendo ésta producto de las operaciones realizadas por cada una de sus dependencias.

Los continuos cambios a los cuales deben enfrentarse las entidades obligan a sus representantes a tomar decisiones de manera cada vez más acertada y oportuna. Este proceso puede resultar bastante complejo si consideramos aspectos tales como la cantidad de factores que están relacionados a una toma de decisión, el volumen de la información requerida, el número de personas que deben participar en el proceso y el grado de incertidumbre propio de cada decisión, entre otros. [3]

Es en este contexto en que se torna vital que las organizaciones cuenten con un proceso analítico estructurado y formal, que facilite el proceso de toma de decisiones, integrando e involucrando a las distintas áreas responsables y creando consensos al interior de la empresa. Para que dicho proceso genere decisiones alineadas con los objetivos estratégicos de la organización, es esencial que los sistemas de información también estén integrados, ya que ello puede proporcionar mayor confianza y flexibilidad para enfrentar las distintas barreras que pueden surgir en la toma de decisiones. [3]

En cuanto a la importancia de la información para las entidades, existen personas no autorizadas que pretenden acceder a ella con fines dañinos, cada día desarrollan sus destrezas y habilidades para poder evadir las protecciones establecidas y lograr su cometido ocasionando daños en los sistemas de información.

La respuesta a estas actividades ilícitas, por parte de los actores encargados en custodiar la información organizacional consiste en implementar procesos de seguridad a los sistemas informáticos, estableciendo barreras protectoras que impida permisos de accesos no permitidos de la información, de igual manera software de detección en caso de que terceros logren atravesar los controles implementados.

La seguridad informática, tiene como objetivo principal ofrecer un alto nivel de respaldo de los datos, partiendo desde un documento de políticas y modelos de seguridad para que cada uno de los actores involucrados las cumpla en su totalidad y de esta manera minimizar los riesgos de un ataque que puede ser interno o externo.

La seguridad informática es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. De todas formas, no existe ninguna técnica que permita asegurar la inviolabilidad de un sistema. Un sistema informático puede ser protegido desde un punto de vista lógico o físico. Por otra parte, las amenazas pueden proceder desde programas dañinos que se instalan en la computadora del usuario. [4]

7.3 NORMA TÉCNICA ISO/IEC 27001

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2. [5]

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001. [5]

El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo).Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente. [5]

Figura 2. Estructura de ISO 27001

7.4 MARCO LEGAL

LEY 1273 DE 2009

"Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "De la Protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones" [6]

Capítulo primero:

-Artículo 269A: Acceso abusivo a un sistema informático.

– Artículo 269b: obstaculización ilegítima de sistema informático o red de telecomunicación.

–Artículo 269c: Interceptación de datos informáticos

– Artículo 269D: Daño informático

– Artículo 269E: Uso de software malicioso

– Artículo 269F: Violación de datos

-Artículo 269G: Suplantación de sitios web para capturar datos personales.

– Artículo 269I: Hurto por medios informáticos y semejantes.

– Artículo 269J: Transferencia no consentida de activos.

8. DESARROLLO E IMPLEMENTACIÓN

8.1 Misión

A través de la Gestión Administrativa lograremos el mejoramiento continuo de la calidad de vida de sus habitantes, garantizando la prestación de los servicios que demanda la comunidad desde el ejercicio de una Administración eficiente con procesos de Planeación, Organización, Dirección, Ejecución y Control, con énfasis en la calidad de los servicios y procurando un

desarrollo Socio-económico sostenible ambientalmente y con plena Participación y liderazgo Ciudadano enmarcada en los principios constitucionales. [7]

8.2 Visión

Ser en el 2020 un Municipio participativo, autosuficiente, sostenible con identidad cultural y sentido de pertenencia por lo nuestro, con desarrollo agroindustrial, turístico y humano protegiendo el medio ambiente, elevando la calidad de vida de la población, con una administración inteligente, ágil, eficiente y transparente. [7]

8. 3 GESTIÓN DE ACTIVOS

En la alcaldía Municipal de Paratebueno se cuenta con los siguientes activos de información físicos en la planta física y dependencias de esta entidad:

DEPENDENCIA	CANT	OBJETO	MARCA	SERIE	ESTADO		
					B	R	M
PLANEACIÒN SISBEN	1	COMPUTADOR DE MESA BLANCO	LENOVO	P900EAMJ	X		
SECRETARIA DE SALUD Y EDUCACION	1	MONITOR DE MESA	LENOVO	OMO4711B1650579	X		
SECRETARIA DE SALUD Y EDUCACION	1	TORRE CPU	LENOVO	ESO7620007		X	
SECRETARIA DE SALUD Y EDUCACION	1	MONITOR DE MESA	AOC	K7387CA000598		X	
SECRETARIA DE SALUD Y EDUCACION	1	TORRE CPU	ONLINE INTEL			X	
SECRETARIA DE SALUD Y EDUCACION	2	COMPUTADORES TODO EN UNO	LENOVO	CS01814789 - CS01810903	X		
SECRET. HACIENDA CONTABILIDAD	1	COMPUTADOR DE ESCRITORIO	LENOVO C40-30	P900EAH8	X		
SECRET. HACIENDA CONTABILIDAD	1	COMPUTADOR DE ESCRITORIO	HP			X	
SECRET. HACIENDA CONTABILIDAD	1	TECLADO	GENIUS	WE0592064443	X		
SECRET. HACIENDA CONTABILIDAD	1	MOUSE	LENOVO	3GB47E0451B	X		
SECRET. HACIENDA CONTABILIDAD	1	CPU CON CABLE	JANUS	6MYYH-4RJ8J-X3CGV	X		
SECRET. HACIENDA CONTABILIDAD	1	TECLADO	LENOVO	50328142	X		
SECRET. HACIENDA CONTABILIDAD	1	MOUSE	LENOVO	150401454984	X		
SECRET. HACIENDA CONTABILIDAD	1	COMPUTADOR PORTATIL	DELL	Q82-CX97			
SECRET. HACIENDA CONTABILIDAD	1	COMPUTADOR TODO EN 1 NEGRO	LENOVO		X		
SECRETARIA DE PLANEACIÓN	1	COMPUTADOR PORTATIL	DELL	S/N: BNGXBV1 - 25847486029	X		
SECRETARIA DE PLANEACIÓN	1	COMPUTADOR DE ESCRITORIO COMPLETO (MONITOR, CPU, TECLADO, MOUSE)	LENOVO	SERIAL: P900EAHH	X		
SECRETARIA DE PLANEACIÓN	1	COMPUTADOR PORTATIL	DELL INSPIRON 3420	S/N: SOLW9V1 10920689389	X		
SECRETARIA DE PLANEACIÓN	1	COMPUTADOR TOSHIBA LEADING INNOVATION- Procesador Procesador lntel® CoreTM 17-3612QM	TOSHIBA	SERIAL No. YC414493Q		X	
SECRETARIA DE PLANEACIÓN	1	COMPUTADOR DE ESCRITORIO COMPLETO (MONITOR, CPU, TECLADO, MOUSE), SERIAL: P900EAEP, MARCA LENOVO, MODELO C40-30, 2553000121 CODIGO DE INVENTARIO	LENOVO	P900EAEP	X		

SECRETARIA DE PLANEACIÓN	1	PORTATIL MARCA DELL INTEL CORIE 13.	DELL INSPIRON 3420	8681761261 S/N 3ZKW9V1	X		
CONTRATACIÓN	1	COMPUTADOR DE MESA	LENOVO	CSO1810894	X		
CONTROL INTERNO	1	COMPUTADOR DE ESCRITORIO COMPLETO	LENOVO	CS01810847	X		
SECRETARIA DE HACIENDA	1	EQUIPO DE COMPUTO ALL IN ONE THINKENTRE M72Z	LENOVO	IS3554H5SMJ76RT5	X		
SECRETARIA DE HACIENDA	1	EQUIPO DE COMPUTO ALL IN ONE THINKENTRE M72Z	LENOVO	IS3554H5SMJ76RH7	X		
SECRETARIA DE HACIENDA	1	EQUIPO DE COMPUTO ALL IN ONE THINKENTRE M72Z	LENOVO	IS3554H5SMJ76RT5	X		
SECRETARIA DE HACIENDA	1	COMPUTADOR TODO EN UNO	HP-205 G2	4CE6290FXX	X		
ALMACEN	1	COMPUTADOR TODO EN 1	LENOVO	S/N CS01811807	X		
FAMILIAS EN ACCIÓN	1	PORTATIL	DELL			X	
FAMILIAS EN ACCION	1	COMPUTADOR TODO EN 1	LENOVO		X		
DESPACHO ALCALDE	1	COMPUTADOR DE ESCRITORIO COMPLETO MARCA LENOVO (MONITOR S/N 01809241, CPU, TECLADO Modelo No LXH-EXB-10YA -, MOUSE MARCA GENIUS S/N: X4E87619203837,	LENOVO	S/N 01809241,	X		
DESPACHO ALCALDE	1	COMPUTADOR DE ESCRITORIO COMPLETO MARCA PHONE (MONITOR , CPU, TECLADO MOUSE	PHONE		X		

Tabla 1. Gestión Activos físicos

Al realizar el inventario de activos físicos de información se estableció que los computadores presentan diferentes características y que algunos computadores no ofrecen un buen rendimiento de acuerdo a las tareas a cargo de cada empleado.

Se cuenta con computadores con características de 4 Gigas hasta 8 Gigas en memoria RAM, discos duros desde 500 Giga hasta 1 Tera, procesadores desde Core i3 Dúo hasta Core i5 de 3era generación, Procesador lntel® CoreTM.

Esta entidad no cuenta con un área de sistemas que ofrezca servicio de soporte y mantenimiento de manera inmediata y continua en las diferentes secretarias y oficinas de la entidad, este servicio es contratado con personal o empresas externas.

La mayoría de los equipos de la Alcaldías están marcados con un serial de identificación, el cual se encuentra relacionado en el inventario de Almacén, de esta manera se tiene un control sobre los activos.

8. 4. POLÍTICAS DE SEGURIDAD INFORMATICA EN LA ALCALDIA MUNICIPAL DE ´PARATEBUENO CUNDINAMARCA.

La Alcaldía Municipal de Paratebueno, establece sus políticas de seguridad fundamentadas en los dominios de controles señalados en la norma NTC/IEC ISO 27001 las cuales se relacionan a continuación:

8.4. 1 Política general de seguridad de la información.

Estas políticas van dirigidas a todo el personal de nómina, contratistas y visitantes de la Alcaldía Municipal, el objetivo de estas políticas es que brinden mecanismos que proporcionen directrices, recomendaciones de servicio para optimizar y salvaguardar la Seguridad en la Información del ente territorial, para lo cual se dispondrá en el presupuesto del Municipio del capital necesario que permita implementar un buen desarrollo de las directrices programadas en cada política de seguridad diseñada.

El representante legal y los secretarios de despacho de cada dependencia son garantes de velar por el acatamiento de dichas políticas de seguridad. En caso que las políticas no sean claras y de fácil entendimiento se debe acudir a la oficina del responsable de las Tics en la Alcaldía Municipal.

8.4.2 Política de Uso de Sitios de Trabajo

Estas políticas van dirigidas a todo el personal de nómina, contratistas y visitantes de la Alcaldía Municipal de Paratebueno, con la cual se pretende definir los comportamientos esperados, para minimizar la manifestación de eventualidades que perjudiquen la seguridad en la información de la entidad.

El representante legal y los secretarios de despacho son los garantes de velar por el acatamiento de estas políticas. En dado caso que las políticas no sean claras y de fácil entendimiento se debe acudir a la oficina del responsable de las Tics en la Alcaldía Municipal.

Los controles y normas en las estaciones de trabajo, son:

- Los sitios de trabajo de la Administración Municipal de Paratebueno deben estar protegidos por software antivirus, el cual este habilitado para actualizarse automáticamente. Los usuarios de las oficinas no están autorizados a deshabilitar este control.
- Los sitios de trabajo de los funcionarios convienen permanecer ordenados y limpios, libre de documentación después de horas laborales o falta de permanencia en la oficina por parte del servidor, con la finalidad de evitar el acceso no autorizado por parte de terceras personas.
- El acceso a sitios de trabajo debe ser mediante el uso de usuario y contraseña única de cada empleado, el intercambio de usuarios y contraseñas está prohibido bajo cualquier incidente. Debe hacerse un buen uso de contraseñas, evitando su divulgación, se debe hacer cambio de contraseñas periódicamente.

- Los usuarios tienen la responsabilidad de bloquear la sesión en su computador en el período en que se ausenten de su escritorio, la cual se desbloqueara únicamente con la contraseña del usuario correspondiente. Al finalizar la jornada laboral, se debe cerrar todos los programas apagando los equipos completamente y desenchufados de la corriente.

- Desde la Secretaría General y de Gobierno se debe garantizar la ejecución de las copias de seguridad automatizando el procedimiento por medio de herramientas software con los cuales cuenta la entidad.
- La Secretaría General y de Gobierno debe realizar intentos vigilados de copias de seguridad y de esta manera asegurar que pueden ser correctamente leídas y restauradas.

- El uso en las copias de seguridad de archivos utilizados, protegidos por usuarios de manera individual es responsabilidad excepcional de este. Los usuarios entregaran periódicamente al jefe de oficina el Backup para su registro y resguardo de datos e información.

- Ningún usuario deberá desinstalar, desactivar o manipular aplicaciones o software que no haya sido instalado por soporte técnico; teniendo en cuenta que esto produce un riesgo alto de seguridad para la información de le entidad.
- Se prohíbe que los usuarios manipulen las piezas internas de hardware de los equipos con los cuales cuenta en su lugar de trabajo.
- No se permite por ninguna circunstancia la creación y difusión de software malicioso dentro de la entidad, los usuarios no podrán escribir, compilar, copiar, propagar,

ejecutar de forma intencionada en los dispositivos de le Alcaldía Municipal, programas diseñados para dañar o entorpecer el desempeño de los sistemas de información.

- Hacer buen uso del servicio de navegación a internet, el cual está destinado para apoyar la realización de las actividades laborales asignadas a su cargo. Es por esto que fomenta el autocontrol por parte del servidor público para hacer buen uso de este servicio. Cuando se identifiquen casos del mal uso del internet, al empleado se le hará seguimiento, las debidas restricciones y si la secretaria general y de Gobierno considera se le acarreara las sanciones a lugar.
- Se debe hacer buen uso del correo electrónico institucional en la Alcaldía Municipal de Paratebueno se debe utilizar exclusivamente para temas del trabajo. Los usuarios de los correos electrónicos institucionales no deben enviar mensajes personales, dañinos, relacionados con actividades ilegales y no éticas, que afecten la imagen y buen nombre de la Administración Municipal.
- Los usuarios deben abstenerse de hacer uso de una cuenta de correo electrónico perteneciente a un compañero de trabajo, en dado caso de no encontrarse trabajando, permisos o licencias, se debe implementar el mecanismo de redirección de mensajes, toda información de carácter institucional debe ser enviada a través de una cuenta institucional, correos personales no serán tenidos en cuenta.

- En caso de presentarse fallas, inconvenientes en los sitios de trabajo, se deberá contactar al soporte técnico de la Alcaldía Municipal a través de la Secretaria General y de Gobierno.

8.4.3 Política de Respaldo y Recuperación de datos

La Alcaldía Municipal considera imprescindible la información como activo y es responsabilidad de todos los usuarios de la entidad hacer buen uso de ella y protegerla. La información almacenada en los servidores, dispositivos, equipos de comunicaciones, debe ser resguardada para evitar perdida de información en caso de daños o de fallas. Se debe definir el sistema, el contenido a respaldar, el tipo de respaldo, el medio, la frecuencia y la ubicación. Esta información es definida por la persona a cargo del proyecto, con el apoyo de la Secretaria General y de Gobierno.

- Los backups de los sistemas de información deben ser conservados por un tiempo límite que puede ser de seis meses. Este tiempo es definido por la persona a cargo del proyecto, en coordinación con la Secretaria General y de Gobierno, después de cumplido el tiempo de custodia, los backups pueden eliminarse.
- Se deben construir instrucciones sensatas para la destrucción o reutilización positiva de los medios que contengan información confidencial. Los procedimientos para la eliminación deben ser conforme a la importancia de la información, los cuales son definidos por la persona a cargo del área de sistemas.
- Las áreas donde se recopilan los backups deben áreas seguras. Por esta razón no se debe permitir el ingreso de personal no autorizado, los medios de almacenamiento de los backups no deben ser operados por personas que no estén autorizadas.

- Cuando se presente casos de realizar cambios o actualizaciones sobre algún sistema de información, se debe realizar antes un backup. Lo cual debe estar estipulado en el proceso de gestión de cambios de la entidad.

8.4.4 Política de seguridad Física y Ambiental

La seguridad física y del entorno es parte esencial en la protección de la información y de los aplicativos involucrados en el procesamiento de la seguridad física. Es por esto que es importante definir parámetros que garanticen que todos los empleados públicos de la Alcaldía Municipal apoyen y velen por la integridad y buen uso de los controles implementados.

- Control de acceso utilizando carnets de identificación, todos los empleados públicos, Contratistas deben portar el carnet en un lugar visible que los certifique que laboran para la Alcaldía Municipal de Paratebueno, no se debe permitir entrar a las áreas u oficinas donde no cuenten con la autorización pertinente. El personal de seguridad debe estar atento a personas que no lo porten el carnet y hacer las exigencias del mismo. Si un empleado por olvido no trae su carnet puede hacer uso de uno temporal, se debe realizar el ingreso en planillas o bitácoras del personal diariamente.
- Las oficinas de la Alcaldía Municipal deben contar con dispositivos que controlen el acceso como lo son puertas con seguridad, cerraduras, método de alarmas o controles biométricos.
- La entidad debe diseñar y gestionar un plan de seguridad física que sea revisado y actualizado cada año. Este plan debe considerar la implementación y administración de los controles de seguridad física que protejan el recurso humano, los activos informáticos y los sistemas en la infraestructura física de la Alcaldía, de amenazas y vulnerabilidades de carácter natural, generadas por el hombre o la naturaleza.
- Se debe identificar y limitar el acceso a áreas restringidas, en el plan de seguridad física de las instalaciones de la entidad. El personal no autorizado no debe entrar a

áreas restringidas, para esto es necesario implementar controles de acceso independientes para estas áreas.

- Se debe implementar controles de acceso a los visitantes o terceras personas, con la respectiva identificación de un documento con foto, registro y acompañamiento. El visitante debe llenar la planilla de registro y reportar el ingreso de computadoras, los cuales deberán ser registrados por parte del personal de seguridad. Los visitantes deben estar siempre acompañados por personal de la entidad mientras se encuentren en las oficinas de la Alcaldía Municipal.

- Los carnets de identificación y contraseñas de acceso deben ser destruidos y borrados cuando se presente la desvinculación de personal, es decir cuando un empleado termine su vinculación laboral, todos los códigos de acceso físico utilizados por esta persona deben ser desactivados. Se debe entregar el carnet a la entidad para proceder a su destrucción.

- Registro de maletas, paquetes, bolsos por parte de los guardias de seguridad deben ser revisados a visitantes y terceras personas, tanto al ingreso como a la salida de la entidad con el fin de identificar posibles circunstancias de pérdida o robo de activos de información.

- Control al ingreso y salida de dispositivos de almacenamiento extraíbles, cualquier dispositivo de almacenamiento extraíble como memorias USB, discos duros externos, deberá ser registrado al ingreso a las instalaciones de la entidad. Su uso temporal debe estar autorizado por el jefe inmediato de la dependencia, y

a su vez con el visto bueno de la persona a cuenta del área de Seguridad de la Información. Lo anterior con la finalidad prevenir riesgos al ser utilizados en los equipos de la entidad.

- Las oficinas de los empleados deben permanecer con llave cuando no se están utilizando. No se permite dejar al alcance documentación sobre los escritorios que contenga información de trabajo. Los computadores portátiles deben permanecer bajo llave o con guayas de seguridad para evitar el riesgo de hurto de dispositivos.
- Los sitios de trabajo y los equipos de cómputo en las áreas seguras deben estar ubicados y protegidos apropiadamente, de acuerdo a la naturaleza de la confidencialidad del asunto y de la información que se maneja. Estos equipos deben tener implementados instrucciones de seguridad que documenten el uso adecuado, con el fin de prevenir y evitar la pérdida de información. Los empleados deben ser supervisados por medio de la tecnología de circuito cerrado de televisión durante las jornadas de trabajo y su estadía en la entidad.
- Las grabaciones de video de los empleados con uso de circuito cerrado de televisión deben ser monitoreadas y almacenadas con los mecanismos de seguridad y disponibilidad convenientes para su observación. Estas cintas deben guardar grabaciones por un tiempo no mayor a dos meses.

- Implementar seguridad al recibir correspondencia y envíos, se deben almacenar en un área restringida y deben estar debidamente registrados y señalizados, con la finalidad de evitar perdida de información y activos.

8.4.5 Política de protección contra Software malicioso

La Alcaldía Municipal contara e implementara una solución corporativa de protección contra el software malicioso o malware que considere adecuada para salvaguardar los activos de información, de acuerdo a lo siguiente:

- Es necesario diseñar, documentar, socializar e implementar manuales de protección contra el software malicioso, se debe socializar instructivos que oriente acerca de las medidas necesarias a desarrollar, cuando se detecte software malicioso en los sistemas de información de la Alcaldía. En los manuales debe estar definido de manera clara las fases de prevención, contención y eliminación del software malicioso.
- Los sitios de trabajo de los empleados de la Alcaldía Municipal deben tener instalados en los equipos de trabajo software corporativo de protección contra el Malware, el cual debe estar configurado para que se actualice de forma automáticamente.
- Los servidores de la entidad deben contar con la instalación de los mecanismos de protección contra el Malware o software malicioso. En caso de no contar con la instalación de software, se deben implementar actividades que aseguren y ofrezcan la protección contra el malware.
- En la entidad los sistemas de información, deben estar protegidos con el software corporativo el cual ofrezca protección contra el malware, los usuarios no cuentan con autorización para hacer cambios o modificaciones en las configuraciones del software, únicamente se podrá llevar a cabo con la autorización del personal con funciones de gestión del servicio.
- En dado caso que los usuarios de los sistemas de información presencien alguna novedad frente al funcionamiento del software corporativo, debe ser informado de carácter

inmediato a la persona a cargo de la seguridad de la información por medio de los canales establecidos, el cual dará una solución pronta a la situación presentada.

8.4.6 Política en Gestión incidentes en la seguridad informática.

Esta política está enfocada a todo el personal que tenga permisos y roles en los sistemas informáticos de la Alcaldía Municipal incluyendo los vinculados laboralmente mediante prestación de servicios. Con la presente Política se constituirá a la normatividad básica de la entidad, será socializada con anterioridad, y la instrumentación de las sanciones convenientes por no cumplir y acatar la política, de igual manera los manuales relacionados con esta.

Debe haber compromiso de parte del representante legal en la gestión de sucesos en seguridad de la informática, debe reconocer y patrocinar la importancia de gestionar los incidentes en seguridad, manifestando su compromiso con el cumplimiento de los objetivos establecidos, la normatividad y reglamentación ajustable para la vigilancia de estas eventualidades.

- Los sistemas de información de la Alcaldía deben contar con la capacidad de registrar y permitir la recolección de información adecuada para determinar las causas de un posible incidente en seguridad de la información con la finalidad de mantener la trazabilidad de un incidente acontecido.

- Los casos pertinentes que conduzcan a una incidencia en seguridad de la información serán informados a la Mesa de Apoyo de la entidad, especificando la eventualidad presentada y serán atendidos de manera confidencial. La mesa de ayuda implantará los mecanismos necesarios para su atención y respuesta oportuna.

- Se deben priorizar los acontecimientos en seguridad presentados, con la intención de ofrecer atención y respuesta apropiada, los cuales están establecidos en la valoración de impacto y atención en seguridad de la información.
- Se debe documentar la evidencia legal pertinente de acuerdo a las eventualidades en seguridad de la información presentados. Esto con el fin de identificar el responsable y la compensación del daño ocasionado e implementar una acción judicial, se llevarán a cabo procedimientos encaminados a recolectar, conservar y demostrar la evidencia de acuerdo a la normatividad vigente en la Alcaldía Municipal.

8.4.7 Política de Seguridad de la Red de Datos

Se deben crear mecanismos de control y seguridad por parte del área de gestión de las tecnologías, los cuales garanticen la disponibilidad de la red de datos y los servicios que esta ofrece, permitiendo la integridad y confidencialidad de los datos entregados.

Las responsabilidades del área de gestión de las tecnologías son:

- Con el objetivo de brindar una adecuada protección de los sistemas de información conectados a la red de datos de la Alcaldía Municipal, es necesario ejecutar y mantener una arquitectura perimetral por capas estableciendo normas de configuración para la observación y control del tráfico entrante y saliente indispensable del entorno de datos de sistemas de información.

- Con el fin de mitigar los riesgos de seguridad agrupados a los dispositivos de red de La Alcaldía Municipal, es necesario deshabilitar los servicios, parámetros y puertos de red que por defecto traen activos y que no se requieren para el funcionamiento del servicio, de igual manera que las interfaces que no se estén utilizando.

- Se debe mantener un adecuado registro en documentos por parte de los administradores de la red de datos, que permita tener trazabilidad de la gestión en la red de datos en la entidad. Igualmente teniendo en cuenta los cambios realizados se debe crear y gestionar backups de la configuración activa para el restablecimiento en caso de presentarse fallas en la red de datos.

- Con el fin de un correcto registro y autorizaciones de conectividad necesarios de los dispositivos que necesiten conectarse a la red de datos de la entidad, se hace necesario notificar al área encargada para su debida autorización. Es responsabilidad de esta área desconectar todos los dispositivos que no cuenten con la aprobación y reportar dicha conexión como un suceso en seguridad de la información y ser inspeccionado.

- Se debe contar con permisos de acceso a la red de datos y los recursos respaldados por la solución perimetral de la entidad, dichos permisos se otorgarán en base a los criterios determinados en la arquitectura de seguridad definida. Estos permisos estarán dirigidos por las áreas de plataforma y seguridad de la información, la cuales realizarán una revisión semestralmente con el fin de garantizar las necesidades institucionales y la integridad del modelo de seguridad de la información.

- Es necesario cifrar a través de mecanismos seguros la información confidencial y sobre la cual debe garantizarse su integridad, durante su transmisión a través de las redes donde el acceso es abierto o sin ningún tipo de restricción.

- Se hace necesario desarrollar mecanismos de registro y monitoreo para la supervisión del tráfico transportado por las redes de datos administradas por la Alcaldía Municipal.

Permitiendo la indagación, análisis y generación de reportes frente a sucesos contrarios que perjudiquen la seguridad informática en el ente territorial.

- Se debe hacer control de las conexiones de acceso remoto, de acuerdo a un esquema supervisado por la persona encargada de la Seguridad y tramitado por la administración del área de plataforma de la Alcaldía Municipal. Las conexiones remotas que se realicen por fuera de la red corporativa, es responsabilidad del servidor público el cual cuenta con los permisos de acceso, con el fin de garantizar el nivel mínimo aprobado de seguridad de la información para el correcto manejo del recurso.

8.4.8 Política de Seguridad en los Servicios de Suministro Eléctrico

- Se debe instalar varios enchufes de energía eléctrica regulada en la Alcaldía Municipal.

- Se debe contar con un sistema de energía permanente como es el caso de adquisición de UPS y plantas dieléctricas, a fin de respaldar el apagado regulado y constante de los dispositivos de computo en la Alcaldía Municipal y de esta manera ofrecer la continuidad de las actividades laborales mientras se restauran las fallas y el correcto funcionamiento del servicio de fluido eléctrico.

- Es necesario contar con pulsadores de emergencias los cuales deben estar situados cerca de las salidas de emergencia en las instalaciones donde se encuentren los equipos de cómputo, facilitando un corte ágil de fluido eléctrico en caso que se dé un incidente grave en el servicio.

- La alcaldía Municipal debe contar con salvaguardia contra descargas del fluido eléctrico en las instalaciones de esta entidad.

9. CONCLUSIONES

- Con la realización de este proyecto se concluye que, al no tener un marco de políticas de seguridad definidas, se hace fundamental que se acaten los lineamientos y reglas establecidas en los manuales de la seguridad en la informática y asimismo no estar expuestos a ataques de robo y pérdida de información.
- Con el desarrollo de este trabajo de políticas de seguridad se diagnosticó áreas vulnerables en la entidad, el área de acceso e ingreso de personas a las instalaciones, y vulnerabilidades en las estaciones de trabajo por acceso no autorizado de terceras personas.
- La implementación de los mecanismos y controles sugeridos permiten al representante legal organizar la seguridad con los objetivos principales de la Alcaldía, estableciendo lineamientos que apoyen su gestión y permitiendo reducir la aceptación del riesgo a un nivel mínimo.
- Entregadas las políticas de seguridad de la informática en la Alcaldía del Municipio, permitirán el mejoramiento continuo de los diferentes elementos que lo componen, por tanto, es preciso sensibilizar a los empleados públicos con dichas políticas de seguridad para que participen y apoyen el cumplimento de las mismas.

10. RECOMENDACIONES

- La Alcaldía Municipal debe implementar capacitaciones de sensibilización a los servidores públicos del ente territorial referente a los aspectos transcendentales de la seguridad de la información.
- La entidad debe implementar a mediano plazo el sistema de Gestión de Seguridad de la Información para salvaguardar el activo más importante como lo es la información.
- Es importante que la Alcaldía de Paratebueno apoye la creación de la oficina de Sistemas para facilitar la respuesta y solución por parte de profesionales en sistemas de los incidentes presentados en las áreas de trabajo.
- Se sugiere que se adopte por parte de la entidad en la mayor brevedad posible las políticas de seguridad diseñadas en este proyecto.

10. REFERENCIAS

[1] c. jaime, «El valor de la información para la toma de desiciones,» *Gerencia,* 2012.

[2] P. J. P. y. M. Maria, «Definicion de seguridad informatica,» 2008. [En línea]. Available: https://definicion.de/seguridad-informatica/.

[3] Antonio Jose Segovia, «27001 academy,» [En línea]. Available: https://advisera.com/27001academy/es/que-es-iso-27001/.

[4] Daccach jose camilo, «Delta asesores,» [En línea]. Available: https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/.

[5] Municipio de Paratebueno, «Alcaldia Municipal Paratebueno,» 2013. [En línea]. Available: http://www.paratebueno-cundinamarca.gov.co/.

[6] J. Caiceo, «El valor de la información para la toma de decisiones,» *Revista Gerencia,* 2012.

[7] J. P. P. y. M. Merino, 2008. [En línea]. Available: https://definicion.de/seguridad-informatica/.

[8] blogspot.com.co/, «Evolución de la seguridad informática,» 26 septiembre 2017. [En línea]. Available: http://melopelantodos.blogspot.com.co/2017/09/evolucion-de-la-seguridad-informatica.html.