UNIVERSIDAD HISPANOAMERICANA

CARRERA DE INGENIERÍA INFORMÁTICA

PROYECTO PARA OPTAR POR EL GRADO DE LICENCIATURA

DISEÑAR UN PLAN PARA LA NORMATIVA DEL MICITT EN CIBERSEGURIDAD PARA EL DEPARTAMENTO DE TECNOLOGIAS DE INFORMACION DE LA MUNICIPALIDAD DE MIRAMAR CANTÓN MONTES DE ORO – COSTA RICA 2022

ESTUDIANTE:

TONY GUTIERREZ RODRIGUEZ

CÉDULA: 604180080

JULIO, 2022

TABLA DE CONTENIDO

DECLARACIÓN JURADA

DECLARACIÓN JURADA

Yo Tony Andrey Gutiérrez Rodríguez , mayor de edad, portador de la cédula de identidad número 6-0418-0080 egresado de la carrera de Ingeniería en Informática de la Universidad Hispanoamericana, hago constar por medio de éste acto y debidamente apercibido y entendido de las penas y consecuencias con las que se castiga en el Código Penal el delito de perjurio, ante quienes se constituyen en el Tribunal Examinador de mi trabajo de tesis para optar por el título de Licenciatura , juro solemnemente que mi trabajo de investigación titulado: DISEÑAR UN PLAN PARA LA NORMATIVA DEL MICITT EN CIBERSEGURIDAD PARA EL DEPARTAMENTO DE TECNOLOGIAS DE INFORMACION DE LA MUNICIPALIDAD DE MIRAMAR CANTÓN MONTES DE ORO, es una obra original que ha respetado todo lo preceptuado por las Leyes Penales, así como la Ley de Derecho de Autor y Derecho Conexos número 6683 del 14 de octubre de 1982 y sus reformas, publicada en la Gaceta número 226 del 25 de noviembre de 1982; incluyendo el numeral 70 de dicha ley que advierte; articulo 70. Es permitido citar a un autor, transcribiendo los pasajes pertinentes siempre que éstos no sean tantos y seguidos, que puedan considerarse como una producción simulada y sustancial, que redunde en perjuicio del autor de la obra original. Asimismo, quedo advertido que la Universidad se reserva el derecho de protocolizar este documento ante Notario Público.

En fe de lo anterior, firmo en la ciudad de San José, a los veintiocho días del mes de abril del año dos mil veintitrés.

Firma del estudiante

Cédula: 6-0418-0080

CARTA DE APROBACIÓN DEL TUTOR

CARTA DEL TUTOR

Heredia, Costa Rica, 20 Marzo de 2023

Ing. María Isabel Losilla Barrientos
Directora de la Escuela de Ingeniería Informática
Universidad Hispanoamericana

Estimada Directora:

El estudiante **Tony Gutiérrez Rodríguez**, cédula de identidad número **6 0418 0080**, me ha presentado, para efectos de revisión y aprobación, el trabajo de investigación ***"Diseñar un Plan para la Normativa del MICITT en Ciberseguridad para el Departamento de Tecnologías de información de la Municipalidad de Miramar, Cantón Montes De Oro.",*** el cual ha elaborado para optar por el grado académico de **Licenciatura en Ingeniería Informática.**

En mi calidad de tutor, he verificado que se han hecho las correcciones indicadas durante el proceso de tutoría y he evaluado los aspectos relativos a la elaboración del problema, objetivos, justificación; antecedentes, marco teórico, marco metodológico, tabulación, análisis de datos; conclusiones y recomendaciones.

De los resultados obtenidos por el postulante, se obtiene la siguiente calificación:

a)	ORIGINAL DEL TEMA	10%	10%
b)	CUMPLIMIENTO DE ENTREGA DE AVANCES	20%	20%
c)	COHERENCIA ENTRE LOS OBJETIVOS, LOS INSTRUMENTOS APLICADOS Y LOS RESULTADOS DE LA INVESTIGACION	30%	30%
d)	RELEVANCIA DE LAS CONCLUSIONES Y RECOMENDACIONES	20%	20%
e)	CALIDAD, DETALLE DEL MARCO TEORICO	20%	20%
	TOTAL		**100%**

En virtud de la calificación obtenida, se avala el traslado al proceso de lectura.

Saludos,

RUBEN HEVER FALLAS PEÑA (FIRMA)

Digitally signed by RUBEN HEVER FALLAS PEÑA (FIRMA)
Date: 2023.03.20 10:23:57 -06'00'

Ing. Ruben H. Fallas Peña, MSc.

Ing. Rubén H. Fallas Peña, MSc. | Profesor Facultad de Ingeniería Informática Universidad Hispanoamericana | ruben.fallas@uh.ac.cr | Carné CPIC 6702 | Carné COLYPRO 60205

CARTA DE APROBACIÓN DEL LECTOR

CARTA DE LECTOR

San José, 21 de abril, 2023

Universidad Hispanoamericana
Sede Llorente
Carrera de Ingeniería Informática

Estimados señores,

El estudiante GUTIERREZ RODRIGUEZ TONY., cédula de identidad 6-0418-0080, me ha presentado para efectos de revisión y aprobación, el trabajo de investigación denominado "DISEÑAR UN PLAN PARA LA NORMATIVA DEL MICITT EN CIBERSEGURIDAD PARA EL DEPARTAMENTO DE TECNOLOGIAS DE INFORMACION DE LA MUNICIPALIDAD DE MIRAMAR CANTÓN MONTES DE ORO", el cual ha elaborado para obtener su grado de Licenciatura en Ingeniería Informática con Énfasis en Sistemas de Información.

He revisado el contenido analizando, particularmente lo relativo a la coherencia entre el marco teórico y análisis de datos, la consistencia de los datos recopilados y la coherencia entre éstos y las conclusiones; asimismo, la aplicabilidad y originalidad de las recomendaciones, en términos de aporte de la investigación, considerando que, este trabajo cuenta con mi aval para ser presentado en la defensa pública.

Atte.

ING. MARÍA ISABEL LOSILLA BARRIENTOS M.R.I.
Cédula: 1-0663-0662

AUTORIZACIÓN DEL CENIT

UNIVERSIDAD HISPANOAMERICANA
CENTRO DE INFORMACION TECNOLOGICO (CENIT)
CARTA DE AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCION PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DE LOS TRABAJOS FINALES DE GRADUACION

San José, 28 de abril de 2023

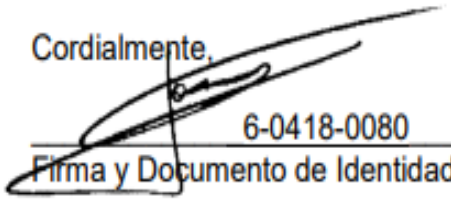
Señores:
Universidad Hispanoamericana
Centro de Información Tecnológico (CENIT)

Estimados Señores:

El suscrito (a) Tony Andrey Gutiérrez Rodríguez con número de identificación 6-0418-0080 autor (a) del trabajo de graduación titulado: DISEÑAR UN PLAN PARA LA NORMATIVA DEL MICITT EN CIBERSEGURIDAD PARA EL DEPARTAMENTO DE TECNOLOGIAS DE INFORMACION DE LA MUNICIPALIDAD DE MIRAMAR CANTÓN MONTES DE ORO presentado y aprobado en el año 2022 como requisito para optar por el título de Licenciatura ; (SI / NO) autorizo al Centro de Información Tecnológico (CENIT) para que con fines académicos, muestre a la comunidad universitaria la producción intelectual contenida en este documento.

De conformidad con lo establecido en la Ley sobre Derechos de Autor y Derechos Conexos N° 6683, Asamblea Legislativa de la República de Costa Rica.

Cordialmente,



6-0418-0080
Firma y Documento de Identidad

DEDICATORIA

Este proyecto es el resultado de años de dedicación, esfuerzo y perseverancia. Y aunque ha sido un camino lleno de desafíos, también ha sido un camino lleno de alegrías y aprendizajes. Y hoy quiero agradecerte a ti madre, por haber sido mi fuente de inspiración y motivación para llegar hasta aquí.

Gracias por tu incondicional apoyo, tus palabras de aliento y tus interminables oraciones. Tú has sido mi roca, mi ejemplo a seguir y mi mayor motivación en cada etapa de mi vida. Nunca te has cansado de creer en mí, y eso es lo que me ha dado la fuerza para seguir adelante incluso cuando las cosas parecían difíciles.

Esta tesis no solo es un logro personal, sino también un homenaje a tu amor, paciencia y dedicación en mi vida. Espero que este trabajo te haga sentir orgullosa de mí, como yo lo estoy de ti. Y aunque las palabras nunca serán suficientes para agradecerte todo lo que has hecho por mí, quiero que sepas que te amo y que siempre te llevaré en mi corazón.

Con todo mi amor y gratitud, Tony Andrey Gutiérrez Rodríguez.

AGRADECIMIENTO

Querida familia, no hay suficientes palabras para expresar lo agradecido que estoy por su amor, apoyo y paciencia durante todo este tiempo en que trabajé en mi tesis. Han sido mi roca, mi motivación y mi fuente de inspiración en cada etapa de mi vida.

A mi madre y padre, quiero agradecerles por haberme inculcado valores como la perseverancia y la dedicación desde pequeño. Sin su amor, guía y sacrificio, no estaría aquí hoy, celebrando la culminación de este proyecto. A mi esposa por estar siempre allí para mí, escuchándome y haciéndome reír, aún en los momentos más difíciles.

Gracias por su apoyo constante y por ser parte de mis mayores logros. Sé que siempre han estado presentes en cada uno de mis logros y en las situaciones más difíciles. Me siento muy afortunado de tenerlos en mi vida.

Este proyecto no solo representa mi trabajo y dedicación, sino que también es un testimonio del amor y apoyo inquebrantable de mi familia. Espero haber honrado su dedicación a lo largo de mi vida, y que este logro les haga sentir orgullosos de mí.

De nuevo, gracias por su amor y apoyo incondicional. lo a seguir y mi mayor motivación en cada etapa de mi vida.

UNIVERSIDAD HISPANOAMERICANA
CENTRO DE INFORMACION TECNOLOGICO (CENIT)
CARTA DE AUTORIZACIÓN DE LOS AUTORES PARA LA CONSULTA, LA REPRODUCCION PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DE LOS TRABAJOS FINALES DE GRADUACION

San José, viernes, 2 de junio de 2023.

Señores:
Universidad Hispanoamericana
Centro de Información Tecnológico (CENIT)

Estimados Señores:

El suscrito (a) Tony Gutierrez Rodriguez, con número de identificación 6-0418-0080, autor (a) del trabajo de graduación titulado DISEÑAR UN PLAN PARA LA NORMATIVA DEL MICITT EN CIBERSEGURIDAD PARA EL DEPARTAMENTO DE TECNOLOGIAS DE INFORMACION DE LA MUNICIPALIDAD DE MIRAMAR CANTÓN MONTES DE ORO – COSTA RICA 2022, presentado y aprobado en el año 2023 como requisito para optar por el título de Licenciatura, ☐SÍ / ☒ NO autorizo al Centro de Información Tecnológico (CENIT) para que con fines académicos, muestre a la comunidad universitaria la producción intelectual contenida en este documento.

De conformidad con lo establecido en la Ley sobre Derechos de Autor y Derechos Conexos N° 6683, Asamblea Legislativa de la República de Costa Rica.

Cordialmente,

Tony Gutierrez Rodriguez
6-0418-0080

UNIVERSIDAD HISPANOAMERICANA

ANEXO 1 (Versión en línea dentro del Repositorio)
LICENCIA Y AUTORIZACIÓN DE LOS AUTORES PARA PUBLICAR Y PERMITIR LA CONSULTA Y USO

Parte 1. Términos de la licencia general para publicación de obras en el repositorio institucional

Como titular del derecho de autor, confiero al Centro de Información Tecnológico (CENIT) una licencia no exclusiva, limitada y gratuita sobre la obra que se integrará en el Repositorio Institucional, que se ajusta a las siguientes características:

a) Estará vigente a partir de la fecha de inclusión en el repositorio, el autor podrá dar por terminada la licencia solicitándolo a la Universidad por escrito.

b) Autoriza al Centro de Información Tecnológico (CENIT) a publicar la obra en digital, los usuarios puedan consultar el contenido de su Trabajo Final de Graduación en la página Web de la Biblioteca Digital de la Universidad Hispanoamericana

c) Los autores aceptan que la autorización se hace a título gratuito, por lo tanto, renuncian a recibir beneficio alguno por la publicación, distribución, comunicación pública y cualquier otro uso que se haga en los términos de la presente licencia y de la licencia de uso con que se publica.

d) Los autores manifiestan que se trata de una obra original sobre la que tienen los derechos que autorizan y que son ellos quienes asumen total responsabilidad por el contenido de su obra ante el Centro de Información Tecnológico (CENIT) y ante terceros. En todo caso el Centro de Información Tecnológico (CENIT) se compromete a indicar siempre la autoría incluyendo el nombre del autor y la fecha de publicación.

e) Autorizo al Centro de Información Tecnológica (CENIT) para incluir la obra en los índices y buscadores que estimen necesarios para promover su difusión.

f) Acepto que el Centro de Información Tecnológico (CENIT) pueda convertir el documento a cualquier medio o formato para propósitos de preservación digital.

g) Autorizo que la obra sea puesta a disposición de la comunidad universitaria en los términos autorizados en los literales anteriores bajo los límites definidos por la universidad en las "Condiciones de uso de estricto cumplimiento" de los recursos publicados en Repositorio Institucional.

SI EL DOCUMENTO SE BASA EN UN TRABAJO QUE HA SIDO PATROCINADO O APOYADO POR UNA AGENCIA O UNA ORGANIZACIÓN, CON EXCEPCIÓN DEL CENTRO DE INFORMACIÓN TECNOLÓGICO (CENIT), EL AUTOR GARANTIZA QUE SE HA CUMPLIDO CON LOS DERECHOS Y OBLIGACIONES REQUERIDOS POR EL RESPECTIVO CONTRATO O ACUERDO.

CAPITULO I

PLANTEAMIENTO DEL PROBLEMA

1.1 INTRODUCCIÓN

El exponencial crecimiento tecnológico en comunicación ha representado un reto para las instituciones, propiciando las mejoras constantes en los servicios, manteniendo la calidad y aumentando la rapidez. Muchas instituciones manipulan una base de datos digital amplia, referente a información sensible de sus clientes o asociados, es aquí donde surge la necesidad de implementar medidas en el ámbito de la ciberseguridad; desarrollando un plan estratégico que involucre a todos los sectores de la institución y, por consiguiente, al personal encargado de los mismos para conseguir una óptima gestión de la seguridad cibernética.

Uno de los grandes retos que presentan las instituciones actuales con la digitalización de muchos procesos que antes se hacían de manera remota, es la contención de las amenazas que emanan del ciberespacio, la novedosa plataforma donde la vida de las naciones transcurre más allá del plano físico, pero que se ha demostrado capaz de alterar la realidad en dicho plano. Los ciberataques son una realidad que potencialmente puede destruir en cuestión de horas la economía, las instituciones y las estructuras de los países vulnerables.

La investigación realizada está enfocada en la implementación de las normas de ciberseguridad proporcionadas por el MICITT en la Municipalidad de Montes de Oro, mediante la elaboración de un plan de normas de seguridad digital que permita la capacitación de personal, el análisis de la situación actual de la institución en la detección de alguna amenaza cibernética, así como su nivel de seguridad en cuanto al resguardo de la información considerada sensible, sea propia o de la ciudadanía.

Es por eso que se busca involucrar al departamento de Tecnologías de la Información de la institución con el objetivo de desarrollar de manera óptima las mejoras que se realizarán a las políticas de seguridad digital. Esto con la finalidad de promover un espacio seguro en un mundo de constante amenazas cibernéticas por parte de personas que buscan su beneficio a partir de perjudicar a entidades, personas e incluso naciones.

Es indispensable que las instituciones asuman la responsabilidad de contener las amenazas potenciales y reales, lo que ha derivado que organismos como la Organización de

las Naciones Unidas, la Organización Internacional del Comercio e incluso la Agencia Internacional para la Energía Atómica, adelanten conferencias y convenciones sobre seguridad informática. Constituye un reto de todos y que compete a todos.

1.2 ANTECEDENTES

1.2.1 RESEÑA HISTÓRICA DE LA EMPRESA

La Municipalidad de Montes de Oro es el Gobierno Local del Cantón de Alvarado, integrado por Regidores y Síndicos ya sean propietarios o suplentes, así como también por el alcalde y vicealcaldesa.

En Ley No°42 del 17 de julio de 1915, Montes de Oro se constituyó como el cantón número cuatro de la Provincia de Puntarenas, con tres distritos. Se designó como cabecera la población de Miramar. Montes de Oro procede del Cantón de Puntarenas, establecido este último en Ley No°22 del 4 de noviembre de 1862.

1.2.2 Atribuciones del Gobierno Local

En el artículo 4 del Código Municipal, se establecen las principales atribuciones de la Municipalidad:

a) Dictar los reglamentos autónomos de organización y de servicio, así como cualquier otra disposición que autorice el ordenamiento jurídico.

b) Acordar sus presupuestos y ejecutarlos.

c) Administrar y prestar los servicios públicos municipales

d) Aprobar las tasas, los precios y las contribuciones municipales, así como proponer los proyectos de tarifas de impuestos municipales.

e) Percibir y administrar, en su carácter de administración tributaria, los tributos y demás ingresos municipales.

f) Concertar, con personas o entidades nacionales o extranjeras, pactos, convenios o contratos necesarios para el cumplimiento de sus funciones.

g) Convocar al municipio a consultas populares, para los fines establecidos en esta Ley y su Reglamento.

h) Promover un desarrollo local participativo e inclusivo, que contemple la diversidad de las necesidades y los intereses de la población.

i) Impulsar políticas públicas locales para la promoción de los derechos y la ciudadanía de las mujeres, en favor de la igualdad y la equidad de género.

1.2.3 MISIÓN

La misión es un motivo o una razón de ser por parte de una organización, una empresa o una institución. Este motivo se enfoca en el presente, es decir, es la actividad que justifica lo que el grupo o el individuo está haciendo en un momento dado.

La misión depende de la actividad que la organización realice, así como del entorno en el que se encuentra y de los recursos de los que dispone.

La Misión de la Municipalidad de Montes de Oro, define cuál es su razón de ser, qué está llamada a ser y a hacer en el próximo quinquenio. Remite a las características de su organización, de sus recursos, de sus experiencias, de su entorno social, económico, político, etc.

La misión de la municipalidad de Montes de Oro es la siguiente: “Somos un Gobierno Local que procura el desarrollo integral de sus habitantes y su territorio mediante la gestión de gobierno de puertas abiertas”.

1.2.4 VISIÓN

La visión municipal se refiere a una imagen que la organización plantea a largo plazo sobre cómo espera que sea su futuro, una expectativa ideal de lo que se espera que ocurra. La visión debe ser realista, pero puede ser ambiciosa, su función es guiar y motivar al grupo para continuar con el trabajo. En ella se define, imagina, proyecta o visualiza el horizonte a dónde quiere llegar la municipalidad en el próximo quinquenio.

La Visión de la Municipalidad de Montes de Oro se define de la siguiente manera: “Ser un Gobierno Local que marque la pauta en cuanto a la prestación de servicios, ejecución de recursos y gestión de proyectos”

1.3 JUSTIFICACIÓN

El presente proyecto de investigación pretende conocer y evaluar las medidas de seguridad cibernética utilizadas en la actualidad por el departamento de TI de la municipalidad, apoyándose en el apartado de ciberseguridad del manual de normas técnicas para la gestión y el control de las Tecnologías de Información del MICITT.

La Global Forum on Cyber Expertise (2016) define la ciberseguridad, con un concepto muy completo, de la siguiente manera:

> “La colección de herramientas, políticas, conceptos de seguridad, salvaguardas, guías, enfoques de gestión de riesgos, acciones, entrenamiento, mejores prácticas, seguridad y tecnologías, que pueden ser usadas para proteger los activos de la organización y de los usuarios dentro del ciberespacio” (citado en Romero, 2018, p.9)

De igual manera Bayuk et al (2012, citado en Romero 2018) asegura que la ciberseguridad “tiene que ver con un concepto más amplio, que es la seguridad de la información, definida como la protección de la integridad, confidencialidad y disponibilidad de datos, independientemente de dónde se procesen, transmitan o almacenen (p.10)”.

Por lo anterior citado, se puede afirmar que el concepto de ciberseguridad implica todas aquellas acciones que se realicen para prevenir, detectar, minimizar y resguardar información y documentación sensibles de las instituciones y de los usuarios que se vean involucrados en las actividades o sistemas de información implementados por las mismas.

Es importante reconocer que pueden existir ciertas limitantes en cuanto a alcances económicos o de existencia de información, lo cual puede influir en el desarrollo de políticas de seguridad en el área digital, provocando un rezago en la atención o detección de las debilidades existentes en este ámbito.

Al realizarse este proyecto se pretende solventar las necesidades en políticas de seguridad cibernética existentes en la institución, así como, resaltar la importancia de proteger el valor de la información estratégica y crítica de la Municipalidad de Montes de Oro; haciendo hincapié en que aún con el extenso potencial que brinda internet, este también conlleva riesgos, como consecuencia de la permeabilidad de los datos críticos, privados y confidenciales.

Por ende, esta investigación tiene como propósito la realización de un plan institucional de ciberseguridad que le permita a la municipalidad poner en práctica las sugerencias establecidas por el MICITT. Evitando así los delitos cibernéticos y las posibles amenazas, que pueden ser, desde afectar el funcionamiento de los sistemas internos, como

el robo o sustracción de datos sensibles de la población o incluso llegar a afectaciones de índole económico.

Con respecto a la entidad encargada de la regulación y seguridad de este sector, de la normatividad y del planeamiento de estas acciones de manera integral y multisectorial se encuentra el llamado Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICIIT).

Hasta hace unos años, cada sector del gobierno normaba a través de directivas y de manera restringida y sectorizada las actividades orientadas a la protección de la información almacenada en sus data centers. La promulgación de la **DIRECTRIZ N° 133-MP-MICITT** del 21 de abril de 2022 reestructura el panorama en materia de Estrategias Integradas de Ciberseguridad.

Es por esta razón que la investigación toma como base las normativas ya propuestas por el MICITT, redirigiendo su implementación a la situación actual de la Municipalidad con la finalidad de conocer el estado actual de la misma en el área de ciberseguridad, resolviendo las necesidades presentes, identificando las debilidades actuales y posibilitando la optimización constante de las normas de seguridad que le permitan a la institución garantizar seguridad en el manejo de su información y de la de los ciudadanos; aumentando así su desempeño, eficacia y credibilidad social por parte de la comunidad.

1.4 PLANTEAMIENTO DEL PROBLEMA

1.4.1 Problemática

En las últimas décadas, las nuevas tecnologías, los servicios electrónicos y redes de comunicación se han visto cada vez más integrados en nuestra vida diaria. Las empresas, la sociedad y el gobierno dependen del funcionamiento de las tecnologías de la información y comunicación (TIC). Definido por Cabrero (1998, citado en Belloch 2012) como:

> En líneas generales podríamos decir que las nuevas tecnologías de la información y comunicación son las que giran en torno a tres medios básicos: la informática, la microelectrónica y las telecomunicaciones; pero giran, no sólo de forma aislada, sino lo que es más significativo de manera interactiva e interconexionadas, lo que permite conseguir nuevas realidades comunicativas. (p.1)

La implementación de estas nuevas tecnologías propició la creación de un espacio virtual, invisible y amplio, al cual posteriormente se le denominó como el ciberespacio. Según Arbeláez (2017) en su artículo científico *"El Ciberespacio y el problema de la realidad virtual"*, asegura que la primera utilización de la expresión Ciberespacio se encuentra, probablemente, no en los estudios académicos, sino en la literatura, más específicamente, en la novela de ciencia ficción Neuromante de Gibson, publicada en 1984. Gibson utiliza el concepto para referirse "a un espacio digital construido por muchos computadores en red, al que sólo podía accederse desde una terminal personal, mediante goggles y conexiones electrónicas entre el ordenador y el sistema nervioso, que permitía a los usuarios ingresar a una onírica matriz que operaba como una 'alucinación consensual'".

Como resultado, este nuevo espacio ha dado lugar a la aparición de retos cibernéticos, ejemplificados como amenazas creadas por individuos, organizaciones o estados que buscan interactuar de manera negativa con el amplio mar de información existente y beneficiarse de manera ilícita de la misma. Tales acciones pueden identificarse como ataques o amenazas cibernéticas, incluyendo entre estas los virus, botnets y los ataques DDoS; todos desarrollados por individuos denominados hacker.

Estas actividades ilícitas mencionadas anteriormente, pueden causar efectos muy adversos a las víctimas y reportar sustanciales beneficios al perpetrador, quien además muchas veces no puede ser identificado o localizado, dejando impune la acción. Es así que, como respuesta a lo expuesto, nace el concepto de ciberseguridad; buscando prevenir, minimizar y evitar daños por medio de entes cibernéticos externos a las empresas, personas o a nivel nacional.

Por esto, la Municipalidad de Montes de Oro, bajo la supervisión del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), busca la implementación de un plan de ciberseguridad con el objetivo de "establecer las acciones para administrar la seguridad de la información, ciberseguridad debidamente respaldada con la política de seguridad de la información / ciberseguridad y que oriente la disponibilidad de niveles de protección y salvaguarda razonables en atención a requerimientos técnicos, contractuales, legales y regulatorios asociados" (Normas técnicas para la gestión y el control de las Tecnologías de Información, p. 13)

Como una entidad gubernamental, la municipalidad busca el beneficio constante de sus ciudadanos mediante la implementación de normativas de seguridad que sirvan como garantía de seguridad y tranquilidad de sus habitantes. Es así como lo expresa el señor Gustavo Torres, Jefe del departamento de Tecnologías de la Información, en la entrevista realizada el día Lunes 13 de Junio "Actualmente presentamos muchas dificultades para poner en marcha las normativas sugeridas por el MICITT, no obstante, es una prioridad su implementación para la institución con la finalidad de buscar siempre el beneficio de los usuarios" al externar la preocupación presente en la municipalidad por solventar las necesidades de ciberseguridad que puedan existir. Sin embargo, como entidad pública que es, ha tenido que adaptar sus estructuras y marcos normativos para prevenir y enfrentar este nuevo escenario tecnológico donde las fronteras no son claras, y los actores pueden no identificarse claramente.

Es de vital importancia el análisis de la gestión administrativa aplicada hasta la actualidad en los ámbitos referentes a la tecnología, identificando los riesgos potenciales y amenazas que pueden poner en graves dificultades los servicios prestados por la institución. Es importante reconocer el papel de los sistemas de información en un escenario mayoritariamente digital, mas, no se puede ignorar las grandes debilidades que presentan en un ambiente de constante crecimiento y expansión.

Por todo lo anterior expuesto, se pretende con esta investigación implementar un plan de ciberseguridad con base en las normativas sugeridas por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones en la Municipalidad de Montes de Oro para

fortalecer el área de ciberseguridad del departamento de TI de la institución como un departamento fundamental en el funcionamiento institucional.

De la identificación de este problema se desprende la siguiente pregunta de investigación: **¿Cuáles son las necesidades en ciberseguridad presentes en la Municipalidad de Montes de Oro, Puntarenas, en el año 2022?**

Con base en esta pregunta de investigación se pretende elaborar un plan de normas técnicas de ciberseguridad para la Municipalidad de Montes de Oro que permita ejecutar las normativas arrojadas por el MICITT, las cuales permitirán prevenir, detectar, impedir, valorar, evaluar y corregir transgresiones a la seguridad que pudieran generarse al nivel de acceso a sistemas, infraestructura e instalaciones en las que se almacena, procesa y transmite información, previendo que el personal y los proveedores tengan accesos mínimos necesarios para la ejecución de sus funciones; se apliquen controles para proteger la confidencialidad, autenticidad, privacidad e integridad de la información. (MICITT, 2021, p. 13-14)

1.4.2 Problema General

¿Cuáles son las necesidades en ciberseguridad presentes en la Municipalidad de Montes de Oro, Puntarenas, en el año 2022?

1.4.3 Problemas Específicos

- ¿Cuáles son las acciones en seguridad cibernética sugeridas por el MICITT?
- ¿Cuáles son las normativas de ciberseguridad implantadas por la municipalidad al día de hoy?
- ¿Cómo implementar las normativas de ciberseguridad recomendadas por el MICITT en la municipalidad de Montes de Oro?

1.5 OBJETIVOS

1.5.1 OBJETIVO GENERAL

- Elaborar un plan de normas técnicas en ciberseguridad mediante el análisis de las políticas de seguridad cibernética aplicadas en la actualidad para la gestión de la ciberseguridad de la institución.

1.5.2 OBJETIVOS ESPECÍFICOS

• Analizar la situación actual del departamento de TI de la Municipalidad en relación a las normativas del MICITT, con el fin de conocer si están empleando técnicas o estrategias de ciberseguridad.

• Determinar las necesidades primarias que presenta la institución para implementar la normativa, según el análisis de la situación actual.

• Elaborar un plan de ciberseguridad institucional que le permita al departamento de Tecnologías de la Información ejecutar las normas sugeridas por el MICITT en la municipalidad.

1.6 ALCANCES Y LIMITACIONES

1.6.1 ALCANCE

Implementar un proyecto que debe entregarse a las autoridades correspondientes de la Municipalidad de Montes de Oro, donde se pueda acudir cuando alguna vulnerabilidad informática se presente para conocer cómo actuar ante el problema con respecto a la situación actual, de modo que sea posible determinar el estado de la institución. Para esto, se organizará reuniones efectivas presenciales y/o virtuales con representantes de la municipalidad, o bien encuestas con el personal municipal. Esto para recolectar información relevante e identificar los requerimientos en relación a las Tecnologías de Información. Este estudio se va a realizar a partir de la información obtenida y que permita identificar necesidades y puntos críticos, además de las normativas del MICITT para realizar estrategias a seguir para la contingencia del problema, y que va a estar dirigido hacia el apoyo y alineamiento de objetivos, políticas, estrategias y demás planes de la Municipalidad.

1.6.2 LIMITACIONES

- Escasa comunicación para la obtención de información por parte de la Municipalidad de Montes de Oro.
- Falta de disponibilidad del personal en la Municipalidad de Montes de Oro para agendar reuniones con los miembros del equipo de trabajo.
- Carencia de documentación en el área de TI.
- Poco tiempo para realizar todo el Sistema de Gestión de Seguridad de la Información que solicita la Municipalidad de Montes de Oro

CAPITULO II

MARCO TEORICO

Marco Teórico

En este capítulo se contemplan aspectos teóricos referentes al tema en estudio sobre el impacto de la implementación de las normativas planteadas por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, en el departamento de Tecnologías de la Información de la Municipalidad de Montes de Oro.

A continuación, se especifican conceptos relevantes para la investigación, los cuales posibilitan una mejor comprensión de los elementos involucrados en el desarrollo de la misma.

2.1 Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT).

Es el ente rector del sector Ciencia, Innovación, Tecnología, Telecomunicaciones y Gobernanza Digital del Gobierno de la República de Costa Rica.

Generan e impulsan el cumplimiento de las políticas públicas en materia de ciencia, innovación, tecnología y telecomunicaciones del país mediante el ejercicio de la rectoría sectorial y la ejecución efectiva de sus procesos sustantivos y de gestión, para mejorar la competitividad en beneficio del bienestar social, la igualdad y la prosperidad de la sociedad costarricense en el marco de la transformación digital y la cuarta revolución.

También busca ser una herramienta que garantice el cumplimiento efectivo del derecho humano de acceso a la información pública, de forma proactiva, oportuna, oficiosa, completa y accesible.

2.1.1 Funciones

En su artículo 20 indica que el Ministerio de Ciencia,Tecnología y Telecomunicaciones tiene las siguientes atribuciones (2022):

a) Definir la política científica y tecnológica mediante el uso de los mecanismos de concertación que establece el Sistema Nacional de Ciencia y Tecnología, y contribuir a la integración de esa política con la política global de carácter económico y social del país, en lo cual servirá de enlace y como interlocutor directo ante los organismos de decisión política superior del Gobierno de la República.

b) Coordinar la labor del Sistema Nacional de Ciencia y Tecnología por medio de la rectoría que ejerce el mismo ministro de Ciencia, Innovación, Tecnología y Telecomunicaciones.

c) Elaborar, poner en ejecución y darle seguimiento al Programa Nacional de Ciencia y Tecnología, de conformidad con lo que establece esta ley, y en el marco de coordinación del Sistema Nacional de Ciencia y Tecnología.

d) Otorgar, según el caso, la concesión de los incentivos que esta ley establece, mediante la suscripción del contrato de incentivos científicos y tecnológicos, previa recomendación de la Comisión de Incentivos.

e) En consulta con los ministros rectores de cada sector, sugerir el porcentaje del presupuesto que las instituciones indicadas en el artículo 97 de esta ley deberán asignar para ciencia y tecnología, de conformidad con las prioridades del Programa Nacional de Ciencia y Tecnología.

f) Promover la creación y el mejoramiento de los instrumentos jurídicos y administrativos necesarios para el desarrollo científico y tecnológico del país.

g) Apoyar las funciones del Ministerio de Planificación Nacional y Política Económica (MIDEPLAN) en el campo de la cooperación técnica internacional, con el estímulo del adecuado aprovechamiento de ésta en las actividades científicas y tecnológicas.

h) Ejercer la rectoría del sector telecomunicaciones generando políticas públicas que permitan el cumplimiento de los objetivos enumerados en el artículo 2 de la Ley N.º 8642, Ley General de Telecomunicaciones.

i) Como rector del sector telecomunicaciones deberá observar y cumplir los principios rectores enumerados en el artículo 3 de la Ley N.º 8642, Ley General de Telecomunicaciones.

j) Velar por el cumplimiento de esta ley.

k) Cualquiera otra función que la legislación vigente y futura le asignen"

2.2 Seguridad

La Comisión sobre Seguridad Humana de las Naciones Unidas, en su informe final Human Security Now, define la seguridad humana como:

> "…protección del núcleo vital de todas las vidas humanas de forma que se mejoren las libertades humanas y la realización de las personas. La seguridad humana significa proteger las libertades fundamentales, aquellas libertades que son la esencia de la vida. Significa proteger a las personas de situaciones y amenazas críticas (graves) y más presentes (extendidas). Significa utilizar procesos que se basen en las fortalezas y aspiraciones de las personas. Significa crear sistemas políticos, sociales, medioambientales, económicos, militares y culturales que, de forma conjunta, aporten a las personas los fundamentos para la supervivencia, el sustento y la dignidad." (p.4)

Concluyendo así, con la idea de que la seguridad tiene como objetivo, la protección de las vidas humanas y de cualquiera que tenga malas intenciones sobre la misma.

2.3 Ciberseguridad

Según Rea (2020) “se define como la “protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados” (p. 7)

Básicamente, es el área relacionada con la informática que enfocada en la protección de la infraestructura computacional y en la información contenida en un ordenador o circulante a través de las redes de computadoras

Deloitte (2016) plantea algunas de las amenazas más propagadas en la red que intentan romper una o varias de las premisas de seguridad anteriormente descritas:

2.3.1. SPAM

Para Internet el correo basura, correo no solicitado o spam es de uno de los grandes problemas que afronta actualmente Internet, según algunas estadísticas es el 80% de todo el correo electrónico que circula por la Red.

2.3.2 DDoS

Los ataques DDoS tienen como principal objeto obtener un beneficio económico y realizar el máximo daño a nivel financiero, técnico y de reputación, colapsando la red y atacando a los recursos en Internet de forma simultánea y desde varios puntos. Los equipos que generan el ataque se suelen nombrar como “Bots” o “Zombies”.

2.3.3 Botnets

Las características mencionadas anteriormente, así como su bajo coste unido a la gran variedad de formas de explotación, lo convierten en uno de los métodos de acciones ilegitimas o ilegales más importantes en la red. En la actualidad existen redes zombis de unos pocas maquinas hasta redes muy grandes que pueden llegar a implicar cientos de miles de máquinas con unas características muy precisas; todas con una amplia variedad de posibilidades de uso y métodos de explotación.

2.3.4. Fraude

Los intentos de fraude tradicionalmente identificados tienen también presencia en el mundo de Internet, en el que nuevas herramientas y posibilidades de comunicación están también a disposición del timador.

2.4 Seguridad Informática

Según Voutssas M., J. (2010), la seguridad informática es “el proceso de establecer y observar un conjunto de estrategias, políticas, técnicas, reglas, guías, prácticas y procedimientos tendientes a prevenir, proteger y resguardar de daño, alteración o sustracción a los recursos informáticos de una organización”. (p. 131)

Los riesgos y amenazas deben ser administrados para así reducirlos a niveles aceptables, por lo que se garantiza a la empresa el correcto funcionamiento interrumpido de sus actividades y el de los recursos, y de esa manera se permite el logro de sus objetivos.

2.5 Amenaza

Para Quiroz y Macías (2017) “las amenazas consisten en la fuente o causa potencial de eventos o incidentes no deseados que pueden resultar en daño a los insumos informáticos de la organización y ulteriormente a ella misma.” (p.682)

Es decir, una amenaza, en el contexto de la seguridad de la información, se refiere a cualquier cosa que pueda causar un daño grave a un sistema de información; es algo que puede o no puede ocurrir, pero tiene el potencial de causar daños graves.

De igual manera, hacen mención del concepto de *Malware* (Malicious Software o Software Malicioso) el cual es definido como: “programas cuyo objetivo es el de infiltrase en los sistemas sin conocimiento de su dueño, con objeto de causar daño o perjuicio al comportamiento del sistema y por tanto de la organización.” (p.682)

2.6 Riesgo

Según Solarte, Enríquez y Benavides (2015) “los riesgos como las diversas maneras en que se presenta la amenaza y la posibilidad de que ese ataque llegue a presentarse en una organización específica.” (p.497)

Los riesgos de seguridad de la información se pueden expresar como efecto de la incertidumbre sobre los objetivos de seguridad de la información y está asociado con la posibilidad de que las amenazas aprovechen las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización.

Además, la Organización Internacional de Normalización [ISO 27001] (2013) dice que “una empresa puede afrontar el riesgo básicamente de tres formas diferentes: eliminarlo, mitigarlo o trasladarlo.

2.6.1 Eliminar Riesgo

Si el riesgo es muy crítico, hasta el punto de que pueda poner en peligro la propia continuidad de la organización, ésta debe poner todos los medios para tratar de eliminarlo, de manera que haya un posibilidad cero de que la amenaza se llegue realmente a producir.

2.6.2 Mitigar Riesgo

En la gran mayoría de ocasiones no es posible llegar a la eliminación total del riesgo, ya sea porque es imposible técnicamente o bien porque la empresa decida que no es un riesgo suficientemente crítico.

2.6.3 Eliminar Riesgo

Esta opción está relacionada con la contratación de algún tipo de seguro que compense las consecuencias económicas de una pérdida o deterioro de la información.” (p. 11)

2.7 Vulnerabilidad

Para Molina y Orozco (2020) “las vulnerabilidades de los sistemas de información es el resultado de bugs en el diseño del sistema, también puede ser resultado de las limitaciones tecnológicas.” (p.2)

En el contexto de la seguridad de sistemas de la información puede ser un fallo en un sistema que puede dejarlo accesible a los atacantes o también puede referirse a cualquier tipo de debilidad en el propio sistema de información que deje la seguridad de la información expuesta a una amenaza.

2.8 Sistemas Gestión de la Seguridad de la Información(SGSI)

Pretende ser una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información. Esta norma está dirigida a los responsables de iniciar, implantar o mantener la seguridad de la información de una organización.(Silva, Segadas y Kowask, 2014, p.21).

Normalmente la persona que se ocupa de implementar el SGSI dentro de la empresa es responsable de coordinar todas las actividades relacionadas con la gestión de la seguridad de la información en la Organización. En organizaciones pequeñas y medianas, este papel puede asignarse a una sola persona; en sistemas más grandes, es aconsejable asignar este cometido a un grupo de personas

2.9 Confidencialidad

Para Calderón (s.f) “en términos de seguridad de la información, la confidencialidad hace referencia a la necesidad de ocultar o mantener secreto sobre determinada información o recursos.” (p.2)

La confidencialidad, cuando nos referimos a sistemas de información, permite a los usuarios autorizados acceder a datos confidenciales y protegidos. Existen mecanismos específicos garantizan la confidencialidad y salvaguardan los datos de intrusos no deseados o que van a causar daño.

2.10 Integridad

Según Avenía (2017) “este principio garantiza la autenticidad y exactitud de la información en cualquier momento que se solicitó o se envía de un entorno tecnológico en que los datos no han sido alterados o destruidos de forma no autorizada.” (p.31)

Se refiere a la exactitud y consistencia generales de los datos o expresado de otra forma, como la ausencia de alteración cuando se realice cualquier tipo de operación con los datos, lo que significa que los datos permanecen intactos y sin cambios.

2.11 Disponibilidad

Para Vision Solutions (2004) “el acceso de usuarios a aplicativos y/o almacenes de datos que se alojan y ejecutan en sistemas informáticos, los que a su vez acceden a información contenida en ficheros y bases de datos soportados por los diversos entornos operativos de una organización.”

En términos más sencillos es la capacidad de un usuario para acceder a información o recursos en una ubicación específica y en el formato correcto.

2.12 Control de Acceso

La función de un sistema de control de acceso es: “proteger la confidencialidad, integridad y disponibilidad de los recursos mediante mecanismos que dificultan la entrada de usuarios no autorizados a los mismos” (Naranjo, 2010, p.14).

El control de acceso es una forma de limitar el acceso a un sistema o a recursos virtuales. En sistemas de la información, el control de acceso es un proceso mediante el cual los usuarios obtienen acceso y ciertos privilegios a los sistemas, recursos o información.

2.13 Análisis

Para Fernández (2002) el propósito básico del análisis es la identificación de determinados elementos componentes de los documentos escritos: letras, sílabas, lexemas, fonemas, sintagmas, palabras, frases, párrafos, títulos, caracteres, reactivos, secciones, temas, asuntos, medidas de espacio, medidas de tiempo, símbolos, etc. y su clasificación bajo la forma de variables y categorías para la explicación de fenómenos bajo investigación. (p. 37)

2.14 Cortafuegos (Firewall)

Según Ocampo, C (2017) los cortafuegos actúan como las rejas con puntas afiladas y las puertas con una docena de cerraduras; sirven para mantener fuera a los bandidos, es decir, sirven al propósito de prevenir ataques o intrusiones en la red interna por ellos protegida.

2.15 Ciclo de Mejora Continua

Mediante el proceso de mejora continua es posible comprobar la eficacia de los controles o si es necesario cambiar de rango o factor de seguridad, realizando las modificaciones que sean necesarias. (ISO,2013, p.13)

2.16 Business Continuity Management (BCP)

Según ESAN (2016) “se puede definir también como una compilación de procesos que permiten identificar y evaluar los riesgos potenciales que podrían interrumpir la actividad normal en la organización.”

2.17 Business Impact Analysis (BIA)

Se establecen escenarios en los que ocurre un siniestro de tal forma que toda la actividad se ve afectada; se procede a identificar los sistemas afectados y se cuantifica económicamente el impacto. (ESAN, 2016)

2.18 Disaster Recovery Plan (DRP)

Se cuenta con un plan estructurado que posibilite la recuperación los sistemas de información del negocio; se establecen procedimientos para respaldar la operación y apoyar la recuperación ante una incidencia. (ESAN, 2016)

2.19 Business Continuity Plan (BCP)

Consta en la definición de procedimientos precisos para garantizar la continuidad de la operación; se asegura el respaldo de información y recursos para la continuidad de la operación. (ESAN, 2016)

2.20 Personal Information Management Systems (PIMS)

Para La Asociación Española para el Fomento de la Seguridad de la Información (2021) “permiten a los individuos gestionar sus datos personales en sistemas de almacenamiento seguros, locales o en línea y compartirlos cuando y con quien ellos elijan, además que podrían decidir qué servicios pueden utilizar sus datos y qué terceros pueden compartirlos.”

2.21 Malware

Para Malwarebytes (2022) “es un término amplio que describe cualquier programa o código malicioso que es dañino para los sistemas con la intención de sacarle dinero al usuario ilícitamente.

Estos son los malhechores más comunes en la galería de la deshonestidad del malware.

2.21.1 Adware

Es un software no deseado diseñado para mostrar anuncios en su pantalla, normalmente en un explorador. Suele recurrir a un método subrepticio: bien se hace pasar por legítimo, o bien se adosa a otro programa para engañar al usuario e instalarse en su PC, tableta o dispositivo móvil. (Malwarebytes, 2022)

2.21.2 Spyware

Es malware que observa las actividades del usuario en el ordenador en secreto y sin permiso, y se las comunica al autor del software. (Malwarebytes, 2022)

2.21.3 Virus

Es malware que se adjunta a otro programa y, cuando se ejecuta normalmente sin que lo advierta el usuario, se replica modificando otros programas del ordenador e infectándolos con sus propios bits de código. (Malwarebytes, 2022)

2.21.4 Gusanos

Son un tipo de malware similar a los virus, que se replica por sí solo con el fin de diseminarse por otros ordenadores en una red, normalmente provocando daños y destruyendo datos y archivos. (Malwarebytes, 2022)

2.21.5 Troyano

Es uno de los tipos de malware más peligrosos. Normalmente se presenta como algo útil para engañar al usuario. Una vez que está en el sistema, los atacantes que se ocultan tras el troyano obtienen acceso no autorizado al ordenador infectado. Desde allí, los troyanos se pueden utilizar para robar información financiera o instalar amenazas como virus y ransomware. (Malwarebytes, 2022)

2.21.6 Ransomware

Es un tipo de malware que bloquea el acceso del usuario al dispositivo o cifra sus archivos y después lo fuerza a pagar un rescate para devolvérselos. El ransomware se ha reconocido como el arma preferida de los delincuentes informáticos porque exige un pago rápido y provechoso en criptomoneda de difícil seguimiento. El código que subyace en el ransomware es fácil de obtener a través de mercados ilegales en línea y defenderse contra él es muy difícil. (Malwarebytes, 2022)

2.21.7 Rootkit

Es un tipo de malware que proporciona al atacante privilegios de administrador en el sistema infectado. Normalmente, también se diseña de modo que permanezca oculto del usuario, de otro software del sistema y del propio sistema operativo. (Malwarebytes, 2022)

2.21.8 Keylogger

Es malware que graba todas las pulsaciones de teclas del usuario, almacena la información recopilada y se la envía al atacante, que busca información confidencial, como nombres de usuario, contraseñas o detalles de la tarjeta de crédito. (Malwarebytes, 2022)

2.21.9 Cryptojacking

Permite que otras personas utilicen su ordenador para hacer minería de criptomonedas como bitcoin o monero. Los programas maliciosos de minería de criptomonedas utilizan los recursos de su ordenador, pero envían los coins obtenidos a sus propias cuentas, no a las del propietario del equipo. En pocas palabras, un programa de minería de criptomonedas malicioso, le roba recursos para hacer dinero. (Malwarebytes, 2022)

2.21.10 Exploits

Son un tipo de malware que aprovecha los errores y vulnerabilidades de un sistema para que el creador del exploit pueda asumir el control. Los exploits están vinculados, entre otras amenazas, a la publicidad maliciosa, que ataca a través de un sitio legítimo que descarga contenido malicioso inadvertidamente desde un sitio peligroso. (Malwarebytes, 2022)

2.22 Antivirus

Según la empresa en antivirus ESET(2022) lo define como “ un software que detecta y en ocasiones elimina virus informáticos de los dispositivos infectados, y por lo tanto también contribuye a detener la propagación del contenido malicioso; además de combatir una amplia variedad de actividades maliciosas como el espionaje, la grabación de pulsaciones de teclado, el robo de credenciales, el minado no autorizado de criptomonedas, el cifrado no deseado de archivos (por ransomware), la extracción de información (por Troyanos), el correo no deseado (spam) y estafas como otras formas de ciberataques.

CAPITULO III

MARCO METODOLOGICO

En el siguiente capítulo se desarrollará la metodología implementada para la realización de la investigación.

Para Rodríguez (2012):

> La metodología sirve a la ciencia como repertorio prescriptivo de las diferentes etapas y pasos formales que el investigador debe cumplir sucesivamente para procesar los datos obtenidos desde la realidad y alcanzar la verdad o el conocimiento, entendiendo siempre que los hallazgos científicos están caracterizados por la precariedad – es decir, por su carácter provisorio- y por la contractibilidad con la realidad empírica a la que alude.

3.1 Tipo de Investigación

La presente investigación por su finalidad puede clasificarse como una investigación aplicada, descrita por Barrantes (2014) como: “su finalidad es la solución de problemas prácticos para transformar las condiciones de un hecho que nos preocupa”. Siendo el objetivo principal de la investigación conocer la situación actual de la municipalidad de Montes de Oro en términos de Seguridad Informática para posteriormente generar acciones que le permitan crear un cambio regido por las normativas brindadas por el MICITT.

Por su objetivo o profundidad, se clasifica como una investigación descriptiva, partiendo de que la misma describe fenómenos. Se identifican y describen situaciones que acontecen en la actualidad en institución para posteriormente, ser corregidas o mejoradas por parámetros del MICITT.

Así, partiendo del tipo de marco en que tiene lugar, se clasifica como una investigación de tipo de campo ya que "el trabajo de campo es la experiencia constitutiva de la Antropología porque distingue a la disciplina, cualifica a sus investigadores y crea el cuerpo primario de sus datos empíricos". (Stocking, 1993, p. 43)

Esto con la finalidad de realizar el diseño de un plan para la normativa del MICITT en ciberseguridad basado en la Norma ISO 27001, el cual beneficie con su implementación a la municipalidad.

3.2 Enfoque de la Investigación

En este apartado se detallará el enfoque de la investigación, el objetivo esperado a alcanzar por el mismo, además, el instrumento de investigación que será implementado para la recolección de la información por parte de los trabajadores y desarrolladores del departamento de TI de la municipalidad.

La presente investigación presenta un enfoque mixto, el cual puede ser comprendido como un proceso que recolecta, analiza y vierte datos cuantitativos y cualitativos, en un mismo estudio. (Barrantes, 2014, p.100); ya que se utilizan ambos enfoques para obtener información de calidad y precisa.

Según Cook (1979), existen dos métodos para la recopilación de datos: cualitativo y cuantitativo. La distinción más obvia que cabe establecer entre los dos es que los métodos cuantitativos producen datos numéricos y los cualitativos dan como resultado información o descripciones de situaciones, eventos, gentes, acciones recíprocas y comportamientos observados, citas directas de la gente y extractos o pasajes enteros de documentos, correspondencia, registros y estudios de casos prácticos. En el enfoque cualitativo la captura de información nos da la realidad de la seguridad en la institución; a través de la aplicación y análisis de los instrumentos de recolección de información: la observación, las entrevistas y el cuestionario.

Asimismo, tiene un enfoque cuantitativo, debido a que se recopilan y analizan datos de los cuestionarios, para determinar aspectos relacionados con la seguridad de la información.

3.3 Fuentes de Información

De acuerdo con Hernández et al (2006), las fuentes de información son “instancias de donde surgen las ideas de investigación, como materiales, escritos, audiovisuales, teorías, conversaciones, creencias, entre otros” (p. 34).

Las fuentes de información que se utilizaron en esta investigación facultaron el sustento teórico y metodológico del trabajo. Asimismo, permitieron el acceso y ampliación del conocimiento sobre el tema en estudio.

3.3.1 Fuentes Primarias

Hernández et al. (2006) definen las fuentes primarias de la siguiente manera:

> Constituyen el objeto de la investigación bibliográfica o revisión de la literatura y proporcionan datos de primera mano, pues se trata de documentos que contienen los resultados de los estudios correspondientes. Ejemplos de estas son libros, antologías, artículos de publicaciones periódicas, monografías, tesis y disertaciones, documentos oficiales, reportes de asociaciones, trabajos presentados en conferencias o seminarios, artículos periodísticos, testimonios de expertos, documentales, videocintas en diferentes formatos, foros y páginas de internet. (p. 66)

Dentro de las fuentes primarias se encuentra toda aquella información obtenida durante el desarrollo de la investigación con la ayuda de los sujetos en estudio, a los cuales se les realizó cuestionarios y entrevistas.

3.3.2 Fuentes Secundarias

Según Hernández et al. (2006), las fuentes de información secundaria son "listas, compilaciones y resúmenes de referencias o fuentes primarias publicadas en un área de conocimiento en particular, las cuales comentan artículos, libros, tesis, disertaciones y otros documentos especializados" (p. 66).

Las fuentes secundarias que se tomaron en cuenta para el desarrollo de esta investigación fueron la documentación que facilito la institución, tales como resúmenes y libros.

3.4 Sujetos de Información

Nombre Completo	Profesión u Oficio	Experiencia	Puesto Laboral
Gustavo Torres Fernández	Ingeniero Informático	12 años	Jefe del Departamento de TI
Carla Méndez Ramírez	Psicóloga	12 años	Psicóloga
Selma Gonzales Rojas	Administradora	18 años	Tesorera

Arelys Salas Salas	Administradora	5 años	Secretaria del alcalde
Mauren Espinoza Ureña	Secretaria	26 años	Facturación
Milagro Garita Barahona	Administradora	18 años	Jefa de Bienes Inmuebles
Ernesto Murillo Navarro	Ingeniero Topógrafo	6 años	Topógrafo Municipal
María Isabel Corella Castro	Contadora	20 años	Contaduría

Nota: Elaboración propia

3.5 Técnicas y Herramientas de Recolección de Datos

Arias (2006) plantea que los instrumentos son las distintas formas o maneras de obtener la información (p.98). La base fundamental de todo estudio es la recopilación de información, que permita la identificación, observación o proyección de datos sensibles y significativos, los cuales proporcionan a la investigación un fundamento para su realización.

Tal información debe ser recopilada de manera asertiva y rápida, esto con la finalidad de obtener un lote de información amplio, oportuno y completo; procurando la veracidad de la misma. Sin embargo, es de gran importancia cuidar que la selección de información este de acuerdo con el tipo de información buscada para lograr los resultados más favorables y fieles a la naturaleza de la investigación.

Para la recolección de datos se trabajará con las técnicas de encuesta, aplicada a un grupo selecto de trabajadores y desarrolladores del departamento de TI de la Municipalidad de Montes de Oro, la cual permitirá reflejar las necesidades presentes en la institución en

ámbitos como la ciberseguridad y normativas de seguridad general para posteriormente servir de base para el diseño de un plan de normativas para el MICCIT, el cual vendría a resolver en un gran porcentaje las falencias existentes, brindándole a la municipalidad nuevas normativas que le favorezcan es sus labores de seguridad actuales y futuras.

3.5.1 Cuestionario

El cuestionario es un instrumento que incluye una serie de preguntas escritas, las cuales pueden ser resueltas sin intervención del investigador. (Barrantes, 2014, p. 269)

El propósito del cuestionario es conocer la situación actual de la municipalidad en el ámbito de ciberseguridad, así como, las políticas que tienen sobre la misma.

3.5.2 Entrevista

El propósito de la entrevista es conocer el conocimiento que tienen los funcionarios sobre la ciberseguridad en la municipalidad, además de cómo reaccionan ante una posible emergencia.

3.6 Variables

Se manejan variables de tipo cualitativo, las cuales se conocen también como variables categóricas; se caracterizan por no utilizar valores numéricos, sino que describe los datos por categorías o características. (Queestionpro, 2022)

Así mismo, las variables a estudiar se manejan como variables no nominales puesto que no pueden ser clasificadas ni ordenadas lógicamente. No obstante, el proceso de investigación arroja una lógica de desarrollo, la cual permite el desenvolvimiento congruente de las mismas para la conclusión óptima del objetivo principal del proyecto.

A continuación, se presenta una tabla resumen de todas las variables:

Tabla 1. Definición de variables

Objetivos Específicos	Variables	Definición Conceptual	Indicador
Conocer las políticas de ciberseguridad aplicadas en la Municipalidad de Montes de Oro	Políticas de ciberseguridad aplicadas en la municipalidad	Es la búsqueda de las políticas que son aplicadas en la Municipalidad	Falta de políticas en ciberseguridad o políticas mal estructuradas
Analizar la situación actual de la institución en comparación con las normas solicitadas por el MICITT	Normativas del MICITT que utiliza la Municipalidad de Montes de Oro	Es conocer las posibles normativas presentes en la Municipalidad	Falta o pocas normativas para la implementación que requiere el MICITT
Diseñar un plan para fortalecer o mejorar la ciberseguridad en la Municipalidad de	Diseño y desarrollo de protocolos de control	Propuesta donde se especifican algunos controles necesarios para gestionar la	Controles o requisitos aplicables a las vulnerabilidades

Montes de Oro		ciberseguridad	encontradas

Nota: Elaboración propia

Las primeras dos variables permiten la materialización de un panorama situacional actual de la institución en áreas fundamentales para la ejecución del proyecto. Estas, ayudarán a la obtención de una descripción del objeto de estudio, información que posteriormente será clasificada y analizada. Pueden ser catalogadas como variables independientes, puesto que sus valores dependen de sí mismos.

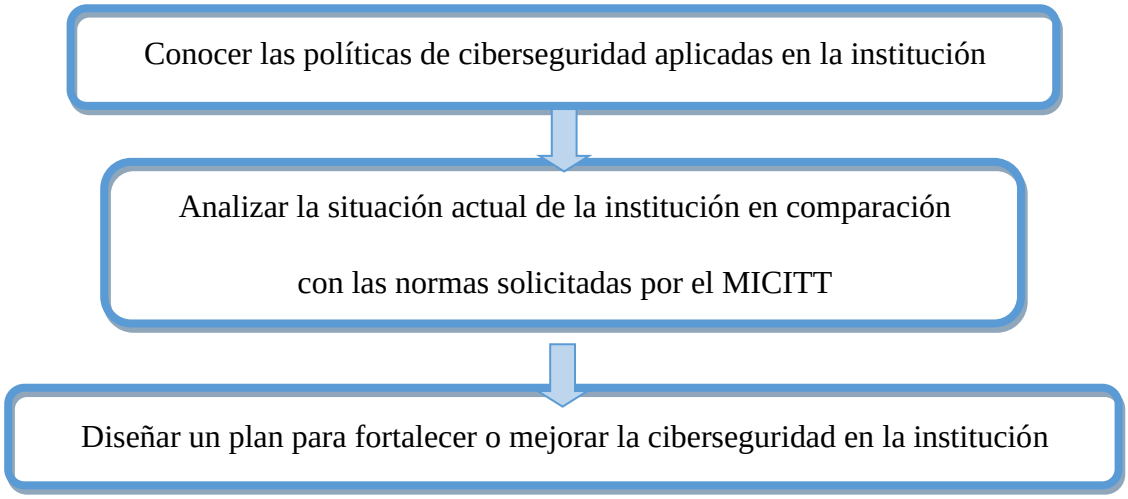
Por otra parte, la variable final puede ser catalogada como una variable dependiente, más específicamente, como una variable respuesta. Esto en tanto, su desarrollo depende estrictamente del análisis, ejecución y estudio de las variables anteriores para, posteriormente, generar una respuesta a la pregunta problema de la investigación.

3.5 Diseño de la Investigación

En esta sección se muestra el diseño y los procedimientos de cada una de las fases ejecutadas para desarrollar la propuesta y encontrar una posible solución a la situación que presenta la Municipalidad de Montes de Oro.

Las fases son definidas en función a los objetivos específicos de la propuesta, facilitando el cumplimiento de cada uno de ellos.

Figura 1. Etapas del diseño de investigación



Fuente: Elaboración propia

3.5.1 Fase 1

Recolección de información. Conocer las políticas de ciberseguridad aplicadas en la municipalidad de Montes de Oro.

Instrumentos:

- Observación
- Cuestionario aplicado al personal pertinente del departamento de TI

3.5.1 Fase 2

Análisis de información. Analizar las normativas del MICITT que utiliza la institución.

Instrumentos:

- Observación
- Entrevista realizada al personal de la municipalidad

3.5.1 Fase 3

Diagnosticar vulnerabilidades institucionales. Hacer un diagnóstico del equipo que utiliza la institución.

3.5.1 Fase 4

Diseñar un plan para fortalecer las normativas y políticas de ciberseguridad de la municipalidad bajo las pautas ya establecidas por el MICITT, mejorando su funcionamiento actual.

3.6 Matriz de Coherencia

La matriz de coherencia es definida por (Marroquin, 2012) un instrumento formado por columnas y filas permite evaluar el grado de coherencia y conexión lógica entre el título, el problema, los objetivos, las hipótesis, las variables, el tipo, método, diseño de investigación, la población y muestra de estudio

En la siguiente tabla se va a observar la relación que existe entre las partes de este proyecto: objetivos específicos, entregables e instrumentos para recolectar datos.

Problema	**Objetivos**	**Hipótesis**	**Instrumentos y variables**	**Metodología**

¿Cuáles son las necesidades en ciberseguridad presentes en la Municipalidad de Montes de Oro? La institución desconoce su estado actual con respecto a las normativas solicitadas por el MICITT	Objetivo General Elaborar un plan de normas técnicas en ciberseguridad mediante el análisis de las políticas de seguridad cibernética aplicadas en la actualidad para la gestión de la ciberseguridad de la institución Objetivos específicos Analizar la situación actual del departamento de TI de la Municipalidad en relación a las normativas del MICITT, con el fin de conocer si están empleando	Diseño de mejoras del plan de políticas de ciberseguridad bajo el desarrollo de un plan de normativas institucionales que cumpla con todos los requisitos del Ministerio de Ciencias y Tecnologías. Para lo que se desarrollará actividades de observación y aplicación de instrumentos de recolección de información que permita conocer el estado actual de la municipalidad en cuanto a políticas y normas de ciberseguridad	Instrumentos de recolección de información Método de la observación Aplicación de un cuestionario Implementación de una entrevista estructurada y semi estructurada Políticas de ciberseguridad presentes en la municipalidad Estudio de la Normativas solicitadas	Implementación del método de observación de campo realizado en las instalaciones propias de la institución Entrevistas semiestructuradas al personal del departamento de TI Cuestionario aplicado a funcionarios de diferentes departamentos que laboran en la institución Diagnóstico de las vulnerabilidades y necesidades en el

	técnicas o estrategias de ciberseguridad. Determinar las necesidades primarias que presenta la institución para implementar la normativa, según el análisis de la situación actual Elaborar un plan de ciberseguridad institucional que le permita al departamento de Tecnologías de la Información ejecutar las normas sugeridas por el MICITT en la municipalidad.	Realizar el análisis de la información obtenida para generar un panorama actual de la situación que presenta la municipalidad en cuanto a vulnerabilidades existentes en su organización y departamento de TI Ofrecer soluciones a las vulnerabilidades observadas y constatadas mediante la respectiva recolección de datos y su análisis para la elaboración de un plan institucional de normativas estructurado	por el MICIITT Diseño y desarrollo de protocolos de ciberseguridad	conocimiento de los colaboradores en el área de ciberseguridad Procesar y analizar la información obtenida, arrojando un panorama crítico de la situación actual Listar las necesidades y vulnerabilidades, proponiendo las soluciones o mejoras y recomendaciones

		bajo las normas del MICITT y el ISO 27001		

CAPITULO IV

DIAGNOSTICO DE LA SITUACION ACTUAL

El objetivo de este capítulo es conocer la situación actual del departamento de Tecnología de Información de la Municipalidad de Montes de Oro en los procesos de la gestión y control de la ciberseguridad, para la implementación de la normativa del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT). Se muestran los procesos actuales sobre cómo se maneja la información.

Para cumplir con los objetivos específicos de este proyecto, específicamente los relacionados con el análisis y diagnóstico, se utilizaron las herramientas de recolección de datos como la entrevista y la observación.

4.1 Diagnostico Administrativo u Operativo

Actualmente, la Municipalidad de Montes de Oro, específicamente el departamento de Tecnologías de la Información, no cuentan con algunos puntos necesarios que requiere la normativa para su implementación.

Se realiza una descripción de los diferentes puntos que no cumple la Municipalidad de Montes de Oro y que son requeridos para la implementación de la Normativa del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT):

- Sistema de Seguridad de la Información (SGSI): Es un documento que tiene como objetivo evaluar todos los riesgos asociados con los datos e información que se manejan en una empresa. La institución no posee un sistema de seguridad de la información, actualmente se encuentra en desarrollo.

- Plan de tratamiento de riesgos de seguridad de la información y privacidad: Es un documento que cuyo fin es el de evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes. No se cuenta con un plan de tratamiento de riesgos, actualmente se encuentra en desarrollo.

- Distribuir todo el software de protección centralmente: Es una forma precisa y rápida de actualizar todos los antivirus para así tener un estándar de protección de todas las computadoras de la institución, actualmente no lo distribuyen de esa manera, sino que lo hacen manualmente una por una.

- No se hacen pruebas periódicas de seguridad: Es un procedimiento que evalúa el nivel de seguridad de una empresa o entidad, analizando sus procesos y comprobando si sus políticas de seguridad se cumplen, en la actualidad la Municipalidad no hace pruebas periódicas de sistemas ni pruebas de penetración de red.

- No se encripta la información: Este es el proceso de codificar un mensaje o información de modo tal que solo los individuos autorizados sean capaces de acceder a esta, y aquellos que no estén autorizados no puedan hacerlo, la Municipalidad de Montes de Oro no encripta la información que almacena, dejándola expuesta para su modificación o extracción.

- No se registran a todos los visitantes al sitio: El departamento de TI no registra a las personas que ingresan a dicho departamento como contratistas, proveedores o personas ajenas a la institución, esto podría resultar en extracción de información o en introducir algún malware a la institución.

- No establecen procedimientos para gobernar la recepción, uso, retiro y desecho de documentos sensibles y dispositivos de salida: Para cualquier empresa es necesario establecer políticas y procesos para tratar los documentos sensibles ya que contienen información que no se debería filtrar además que los dispositivos de salida tienen puertos que podrían vulnerabilidad las computadoras de la institución, dentro de la Municipalidad de Montes de Oro no cuentan con ningún tipo de procedimiento para estos documentos o para los dispositivos de salida.

- No establecen un inventario de documentos sensibles y dispositivos de salida y realizar reconciliaciones periódicas: En la actualidad la Municipalidad de Montes de Oro no cuenta con un sistema de inventario para documentos sensibles ni para dispositivos de salida.

- No usan de forma continua un portafolio de tecnologías, servicios y activos soportados (p. ej., escáneres de vulnerabilidad, fuzzers y sniffers, analizadores de protocolos) para identificar vulnerabilidades de seguridad de la información: Estos son servicios y tecnologías enfocados en conocer el estado de seguridad en que se encuentra una empresa en relación con sus sistemas informáticos, de comunicación y acceso a internet, la institución no identifica las vulnerabilidades que puedan poseer.

4.2 Diagnostico Técnico

4.2.1 Ambiente de Servidores

En este apartado se muestra la infraestructura de servidores que posee la municipalidad de Montes de Oro, para el funcionamiento diario de operaciones. Los servidores con los que cuenta y su función se muestran en la siguiente tabla:

Servidor	Función
Servidor DELL	Servidor de controlador de dominio datos, FTP y chat.

T130	
Servidor HP ML110	Servidor proxy Pfsense.
Servidor Hikvision	Servidor de almacenamiento de video para cámaras IP.
Servidor de telefonía	Central telefónica de telefonía IP.
Servidor HP ML10	Servidor de respaldo de datos.
VPS(alquilado)	Están los programas web, bases de datos, páginas web y aplicaciones web.

4.2.2 Ambiente de las aplicaciones o sistemas

En este apartado se identifican todas las aplicaciones o sistemas necesarios para que la municipalidad opere con normalidad. Estas herramientas pueden ser utilizadas para comunicación, gestión de archivos, procesos específicos, seguridad, entre otros. Seguidamente, se muestra una lista con las aplicaciones y sistemas que utiliza la Municipalidad de Montes de Oro:

1. Microsoft Office: se utiliza todo el paquete, en su mayoría se usa Word y Excel para el desarrollo de informes y otras tareas, en el caso de Excel se utiliza para el control de presupuestos (puesto que no se cuenta con un sistema).

2. Correo electrónico: son los sistemas encargados del manejo de correos electrónicos. Son los medios utilizados para la comunicación interna y externa de la institución y uno de los medios de recepción para la correspondencia de cada departamento, que cuenta con su dirección de correo propia.

3. SICOP: es un modelo de proveeduría virtual, basado en las mejores prácticas internacionales que hace más eficientes los procesos de compra y contratación con las instituciones públicas.

Es la plataforma tecnológica de uso obligatorio de la Administración Central utilizada para llevar a cabo los procesos de contratación administrativa 100% electrónicos y transparentes, el ciclo completo se lleva a cabo por este medio, el mismo posee un registro único de proveedores, el catálogo de bienes y servicios y los expedientes de cada procedimiento.

4. Sim Web: es una herramienta tecnológica de gestión de ingresos proporcionada por el IFAM a varias municipalidades desde 16 de noviembre del 2020, impacta directamente algunas de las actividades de negocio municipales más relevantes, como lo son la gestión de cobro y la recaudación.

5. Google Workspace: es un servicio de Google que proporciona varios productos de Google con un nombre de dominio personalizado por el cliente.

6. ZOOM y Microsoft Teams: ofrecen servicios de videoconferencia basado en la nube que se puede usar para reunirse virtualmente con otras personas, cuando las reuniones en persona no son posibles, ya sea por video, solo audio o ambos, también para actividades como capacitaciones o eventos sociales.

7. SNIT: es la plataforma oficial mediante la cual se publica la información geográfica fundamental de forma estandarizada y siguiendo las normas técnicas utilizadas en la generación de información geoespacial a nivel nacional.

8. Senda: es la herramienta donde el registro público envía las bases de datos sobre movimientos de fincas e hipotecas a nivel nacional.

9. QGIS: es un sistema de información geográfica para la visualización y superposición de diversos tipos de datos (vectoriales e imágenes) en diversos formatos y proyecciones, así como la exploración y composición de mapas usando una interfaz gráfica con una gran variedad de herramientas.

10. Firma Digital: se utiliza para colocar firmas oficiales a documentos sin la necesidad de tenerlos físicamente, sino digitalmente.

11. Valora: es una herramienta informática diseñada para el sector municipal, para determinar el valor de los bienes inmuebles de la jurisdicción municipal en los procesos de fiscalización de las declaraciones y la realización de los avalúos.

12. Autocad: se trata de una potente herramienta con mucha capacidad de edición que permite dibujos en 2D y modelado en 3D.

13. Adobe Acrobat Reader: se utiliza para la lectura de documentos en formato de documento portátil (.pdf), de igual forma es necesario para las firmas digitales.

14. Google Earth Pro: es un sistema de exploración geográfica en tercera dimensión, ofreciendo el conjunto más completo de datos geoespaciales disponibles de manera pública.

15. SIRI: es el Sistema de Información del Registro Inmobiliario, es una herramienta para la interacción, investigación y estudio de los predios comprendidos en el país.

16. MMO.GO.CR: plataforma web para acceder a los sistemas municipales utilizados con más frecuencia.

17. Tesoro Digital: sistema de servicios en línea, que el Ministerio de Hacienda ha puesto a disposición de las entidades públicas que tienen depositados recursos en la Caja Única del Estado.

18. APC: la herramienta digital para tramitación de proyectos de construcción, se utiliza por profesionales para solicitar el sellado ante el Colegio

Federado de Ingenieros y Arquitectos, y específicamente en la municipalidad para obtener el permiso de construcción con convenio.

19. Dolibarr: es un software de Recursos Empresariales y Gestión de Relaciones con los Clientes (GRC, CRM en inglés) para la Pequeña y mediana empresa, autónomos o asociaciones. Se utiliza para elaboración y procesamiento de presupuestos, organiza y controla los pedidos, con seguimiento del flujo de trabajo. También emite los informes y estadísticas de presupuestos y pedidos, tanto de los clientes como de los proveedores.

20. SRD Hidrómetros: es el sistema que se encarga de la lectura de medidores.

21. ATV Hacienda: es el portal de la administración tributaria virtual donde se realizan las declaraciones de impuestos que se presentaban por Tributación Directa.

22. Módulo Internet Banking: este sistema permite a través de Internet, realizar operaciones bancarias.

23. Declara 7: permite capturar y almacenar el registro de los datos del informante y de los detalles, así como la generación de archivos de reporte de la declaración informativa.

24. J-ISIS: es un sistema que permite darle descripción a los archivos físicos de la municipalidad.

25. IVMS-4200: se utiliza para la gestión de los vídeos provenientes de las cámaras de vigilancia.

26. Microsoft Visio: las herramientas que lo componen permiten realizar diagramas de oficinas, diagramas de bases de datos, diagramas de flujo de programas, UML, y más.

27. Google Sketchup: es utilizado para el modelado de entornos de planificación urbana, arquitectura, ingeniería civil, diseño industrial, entre otros.

28. Smart PSS: este software permite la gestión y mantenimiento de las cámaras que se encuentran en el edificio de la unidad técnica y plantel municipal.

29. Plataforma Micitt: una nueva herramienta para aprender en línea, hacer preguntas y recibir respuestas de profesionales en temas de ciencia y tecnología.

30. Anydesk: provee acceso remoto bidireccional entre computadoras personales y se encuentra instalado en todos los equipos de los diferentes departamentos de la municipalidad.

31. Microsoft Windows Defender: es un software antimalware, el cual brinda protección en tiempo real frente a todo tipo de malware y spyware.

32. Mesa de ayuda: es un sistema de tickets para control de tareas municipales.

33. Pfsense: se trata de un servidor, o más bien, un firewall proxy para seguridad de red.

34. Net server: servidor de controlador de dominio y servidor ftp.

35. Zentyal: su función es ser un servidor de respaldos.

36. Hosting VPS: servidor virtual privado, están hospedadas todos las aplicaciones web, como:correos, bases de datos, hospedajes…

37. montesdeoro.go.cr: es el directorio comercial, cultural y turístico del cantón.

38. munimontesdeoro.go.cr: es la página oficial de la municipalidad.

39. VMware: es el programa encargado de virtualizar sistemas físicos en un ordenador.

40. SIM 21: es el sistema antiguo de ingresos, actualmente solo se utiliza para lectura.

41. UniFi: es un sistema que permite integrar las redes Wi-Fi.

42. UNMS: se trata de un software para la administración de antenas inalámbricas.

43. Wordpress: este sistema se encarga de la gestión de contenido web.

44. Ecolones: es la plataforma donde se registran los materiales para reciclaje de esta iniciativa.

45. Sitada: es el resultado del trabajo conjunto de las diferentes dependencias del sector ambiente, y busca establecer un esquema de gestión de la información que sirva de soporte para la toma de decisiones, evaluación y monitoreo del cumplimiento al seguimiento y atención de denuncias ambientales.

Los programas más utilizados son: paquete de Microsoft Office, Adobe Acrobat Reader, Anydesk y la plataforma de correos Gmail. También algunas plataformas son importantes para el trabajo diario del personal como: SICOP, Dolibarr, SIM producción y la firma digital. El gestor de TI realizó una plataforma llamada MMO.GO.CR en la que se encuentran los accesos de las plataformas más utilizadas por los empleados municipales.

4.2.3 Ambiente de redes y telecomunicaciones

La municipalidad de Montes de Oro cuenta con un centro de datos donde se distribuyen datos, video, internet y telefonía IP mediante conexiones inalámbricas privadas con otros edificios como: mercado, CECI, plantel y puntos de vigilancia de la comunidad.

Modelo de dispositivos Red
Switch TP-Link Unidad Técnica

Router conectividad Cisco 1900 series
Router Cisco RV082
Switch HPE OfficeConnect 1620 series
Switch HP ProCurve
Rack ICC
RouterLynksys CECUDI
Punto de acceso UniFiWi-FI
Antena Ubiquiti lite APAC/Litebeam 5AC Anfiteatro
Antena Ubiquiti lite APAC/Litebeam 5AC Linda Vista
Antena CCSS
Antena Ubiquiti lite APAC/Litebeam 5AC IMAS
Antena Ubiquiti lite APAC/Litebeam 5AC Salón Mar Azul
Antena Ubiquiti lite APAC/Litebeam 5AC Guapinol
Antena Ubiquiti lite APAC/Litebeam 5AC Mar Azul CCSS
Antena Ubiquiti lite APAC/Litebeam 5AC Mar Azul Lubricentro
Antena Ubiquiti lite APAC/Litebeam 5AC Servimóvil

Antena Ubiquiti lite APAC/Litebeam 5AC Margarita Penón estación
Antena Ubiquiti lite APAC/Litebeam 5AC Margarita Penónaccesspoint
Antena Ubiquiti lite APAC/Litebeam 5AC Tienda Akari
Antena Ubiquiti lite APAC/Litebeam 5AC Ministerio de Salud
Antena Ubiquiti lite APAC/Litebeam 5AC Escuela JMZB
Antena Ubiquiti lite APAC/Litebeam 5AC Banco Nacional
Antena Ubiquiti lite APAC/Litebeam 5AC Maumbe estación
Antena Ubiquiti lite APAC/Litebeam 5AC Maumbe access point
Antena Ubiquiti lite APAC/Litebeam 5AC Mercado estación
Antena Ubiquiti lite APAC/Litebeam 5AC Mercado accesspoint
Antena Ubiquiti lite APAC/Litebeam 5AC Plantel
Antena Ubiquiti lite APAC/Litebeam 5AC Municipalidad accespoint
Antena Ubiquiti lite APAC/Litebeam 5AC Municipalidad accespoint
Antena Ubiquiti lite APAC/Litebeam 5AC Municipalidad

accespoint
Antena Ubiquiti lite APAC/Litebeam 5AC Ferretería Elizondo estación
Antena Ubiquiti lite APAC/Litebeam 5AC Ferretería Elizondo accesspoint
Antena Ubiquiti lite APAC/Litebeam 5AC Lirios del Valle estación
Antena Ubiquiti lite APAC/Litebeam 5AC Lirios del Valle accesspoint
Antena Ubiquiti lite APAC/Litebeam 5AC Tanque de agua Lirios
Antena Ubiquiti lite APAC/Litebeam 5AC Tanque de agua ZP
Antena Ubiquiti lite APAC/Litebeam 5AC Salón Comunal Santa Rosa
Antena Ubiquiti lite APAC/Litebeam 5AC Salón Comunal San Isidro
Antena Ubiquiti lite APAC/Litebeam 5AC Taller Chavaría
Torre arriostrada de comunicaciones Municipalidad
Torre arriostrada de comunicaciones Plantel

4.2.4 Ambiente de Centro de datos

El espacio destinado al centro de datos en la municipalidad de Montes de Oro, se encuentra dentro de la oficina de TI, donde se localizan con servidores utilizados por la municipalidad. Para entrar al centro de datos es necesario una llave de ingreso, ya que cuenta con una puerta que se mantiene asegurada. Esta llave solo la posee el gestor de TI.

Dentro del centro de datos, los servidores cuentan con protección física del rack donde se encuentran instalados. Además, dentro del lugar se encuentran dos aires acondicionados, el principal y otro de repuesto, para mantener la temperatura de los servidores. Por otro lado, se cuenta con un extintor en caso de presentarse el riesgo de un incendio y con fuentes de poder interrumpible (UPS), que tienen una duración aproximada de 2 horas y media de poder en caso de una interrupción en el suministro de energía a los servidores. También cuenta con una planta de gas que se activa 8 segundos después de que exista ausencia de suministro energético para la municipalidad.

Para añadir más seguridad, el centro de datos tiene una cámara fuera del cuarto, así como sensores para prevenir los daños físicos que alguna persona tenga intención de realizar.

4.3 Diagnostico de Percepción

4.3.1 Actividades realizadas

Las actividades realizadas para la recolección de datos en la Municipalidad de Montes de Oro, con el fin de recolectar datos para implementar la normativa del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), son la observación de los procesos realizados por los funcionarios de la institución, reuniones y entrevistas con el encargado del departamento de TI.

4.3.2 Evaluación de las actividades

Por medio de las reuniones con el encargado del departamento de TI, se comentaron cada uno de los objetivos específicos, con el fin de verificar que los requerimientos propuestos se cumplan a cabalidad, para que la implementación de la normativa se realice correctamente.

4.4 Determinación de Brechas

Del análisis que se obtuvo en este capítulo se pudo encontrar que la Municipalidad de Montes de Oro, tiene brechas que limitan al área de TI poder operar de la manera más optima y que a su vez pueda cumplir sus objetivos y que estos mismos estén alineados con los objetivos de la institución.

Estas son las brechas que se pudieron determinar:

Situación Actual	Brecha	Situación Deseada
La Municipalidad de Montes de Oro no cuenta con un Sistema de Seguridad de la Información (SGSI), ya que actualmente se encuentra en desarrollo.	Debe de existir un Sistema de seguridad de la Información para poder evaluar todos los riesgos asociados con los datos e información que manejan	Contar con un Sistema de seguridad de la Información.
No existe un Plan de tratamiento de riesgos de seguridad de la información y privacidad, actualmente se encuentra en desarrollo.	Debe de contar con un Plan de tratamiento de riesgos de seguridad de la información y privacidad con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes.	Tener un Plan de tratamiento de riesgos de seguridad de la información y privacidad.
No se distribuye todo el software de protección centralmente ya que actualmente se distribuye individualmente en cada computadora de la institución.	Se debe de optar por un software que distribuya al mismo tiempo toda la protección para cada una de las diferentes computadoras de la institución.	Tener un software de protección centralizado, donde se puedan actualizar todas las computadoras al mismo tiempo.
No se hacen pruebas de seguridad, la Municipalidad de Montes de Oro no hace pruebas periódicas de sistemas ni pruebas de penetración de	Deben de realizarse pruebas de sistemas y de penetración de red con el fin de conocer las vulnerabilidades que posean las computadoras y la red de	Realizar pruebas periódicas de sistemas y pruebas de penetración de red para poder conocer si existen vulnerabilidades.

red.	la institución.	
La Municipalidad de Montes de Oro no realiza la encriptación de la información que almacena.	Se requiere encriptar la información que se almacena por fines de seguridad	Realizar la encriptación de la información que almacena.
El departamento de TI no registra a las personas que ingresan a dicho departamento, esto podría resultar en extracción de información o en introducir algún malware a la institución.	Se debe de registrar a cualquier persona que entra al departamento de TI ya que podría extraer o vulnerar la información del departamento.	Registrar a cualquier persona que quiera entrar al departamento de TI y que sea ajeno al mismo.
Dentro de la Municipalidad de Montes de Oro carecen de procedimientos para gobernar la recepción, uso, retiro y desecho de documentos sensibles y dispositivos de salida.	Se deben realizar procesos para tratar los documentos sensibles y también los dispositivos de salida que poseen puertos que podrían generar una vulnerabilidad las computadoras de la institución.	Realizar los procesos necesarios para gestionar de una manera correcta los documentos sensibles y los dispositivos de salida.
La Municipalidad de Montes de Oro no cuenta con un sistema de inventario para documentos sensibles ni para dispositivos de salida.	Se requiere un software de inventario para los documentos sensibles y para los dispositivos de salida ya que no hay un control sobre eso.	Adquirir un software para la gestión y administración del inventario de documentos sensibles y dispositivos de salida.
La institución no identifica las vulnerabilidades que puedan	Se deben implementar las tecnologías y servicios para identificar	Adquirir las tecnologías, servicios y activos para la identificación

poseer ya que no utiliza un portafolio de tecnologías, servicios y activos soportados para identificar estas vulnerabilidades de seguridad de la información.	las vulnerabilidades de la seguridad de la información.	eficiente y eficaz de vulnerabilidades en la seguridad de la información.

Nota: Elaboración propia

CAPITULO V

PROPUESTA DEL PROYECTO

En este capítulo, se toma en cuenta la información de los capítulos anteriores, especialmente los datos recolectados con las herramientas de investigación, las variables y objetivos específicos, así como el diagnóstico de la situación actual.

Se detallará la propuesta con políticas, detallando cada una, con el propósito de conocer las mismas con profundidad.

5.1 Políticas de Seguridad

En este apartado se describen las políticas de seguridad que se utilizaran para un mejor funcionamiento de la institución y respetando las directrices que le solicita el MICITT.

5.1.1 Roles y responsabilidades

A. Descripción General

La identificación de los roles y responsabilidades en la Municipalidad de Montes de Oro, permite establecer al interior de la entidad las acciones correspondientes para proteger los activos de información, reduciendo posibles eventos y/o incidentes de seguridad de la información. De esta manera los colaboradores de la entidad, adquieren el compromiso de protegerlos y se hacen partícipe de las actividades e iniciativas encaminadas al aseguramiento de los recursos que se encuentran bajo su custodia.

B. Propósito

Definir roles y responsabilidades para la atención de incidentes adversos que afecten la seguridad de la información de la Municipalidad de Montes de Oro.

C. Alcance

El presente documento describe los roles y responsabilidades de los encargados de la Seguridad de la información de los diferentes procesos de la Municipalidad de Montes de Oro, conservando la confidencialidad, integridad y disponibilidad de la Información. Por lo anterior, todos los colaboradores de la Municipalidad de Montes de Oro serán responsables de la identificación, evaluación y control de los riesgos de seguridad de la información.

D. Aplicación

Para lograr el buen funcionamiento de la seguridad y privacidad de la Información, la entidad particularizará los roles y responsabilidades de los colaboradores de la entidad que se van a encargar de establecer y desarrollar cada una de estas actividades asociadas a los sistemas.

Para la asignación de los responsables, la Municipalidad de Montes de Oro, analizará las funciones de cada rol relacionándolas con las actividades que realiza el personal de la entidad, por lo anterior, para cada perfil, serán incorporadas los manuales de funciones en las obligaciones de los contratos por prestación de servicios de acuerdo con el cargo que desempeñan.

A continuación, se definen algunos roles y responsabilidades que se deben tener en cuenta en la implantación y seguimiento del Sistema de Gestión de Seguridad de la Información.

- **Comité Institucional de Gestión y Desempeño.**

Como muestra de su compromiso en la dirección, gestión y apoyo en la seguridad y privacidad de la Información, aprueba lo siguiente:

1. Aprobar anualmente o cuando se requiera la Política de Seguridad y Privacidad de la Información de la entidad.
2. Asignar y aprobar el presupuesto necesario para la implantación y posteriormente el normal funcionamiento y/o puesta en marcha del Sistema de Gestión de Seguridad de la Información.
3. Garantizar que los requisitos del Sistema de Gestión de Seguridad de la Información se encuentran integrados en todos los procesos críticos de la entidad.
4. Proporcionar los recursos necesarios para la implementación y desarrollo de las actividades del Sistema de Gestión de Seguridad de la Información en la entidad.
5. Velar por la ejecución y desarrollo de las actividades del Sistema de Gestión de Seguridad de la Información.
6. Promover activamente una cultura de seguridad y privacidad de la información basada en riesgos para la entidad.
7. Aprobar los roles y responsabilidades relacionados con la seguridad de la información en todos los niveles de la entidad.

- **Especialista Seguridad de la Información**

Es el responsable de la Seguridad de la Información en la entidad, el cual debe pertenecer a un área que haga parte de la Alta Dirección. Así mismo, debe pertenecer e informar al Comité Institucional de Gestión y Desempeño todo lo referente al Sistema de Gestión de Seguridad de la Información, al cual asistirá en forma oportuna y garantizará el mejoramiento continuo de cualquier necesidad de mejora respecto a la seguridad y privacidad de la información de la entidad.

1. Emitir conceptos referentes a riesgos y seguridad de la información de la entidad, para la toma de decisiones por parte del Comité Institucional de Gestión y Desempeño.
2. Coordinar la implementación, despliegue y sostenibilidad del Sistema de Gestión de Seguridad de la Información.
3. Mantener una comunicación clara, oportuna, completa y permanente con los diferentes roles.
4. Definir las herramientas, metodologías y lineamientos necesarios para la implementación de la seguridad y privacidad de la Información.
5. Verificar que se incluyan los temas asociados a la seguridad y privacidad de la Información, dentro del plan de capacitaciones de la entidad.
6. Asegurar que se definan e implementen actividades de sensibilización y concienciación frente a la seguridad de la información a la Alta Dirección y demás partes interesadas.
7. Guiar a la Alta dirección de la entidad, ante incidentes de seguridad mediante el plan de respuesta de incidentes.
8. Responsable de la elaboración y desarrollo del Plan de Seguridad de la Información.
9. Mantener contacto con grupos de interés.
10. Mantener y promover la actualización de las políticas de seguridad de la información.
11. Debe responder por la revisión de problemas de seguridad de la información existentes y aquellos que se consideren potenciales.

- **Responsabilidades Colaboradores**

Es responsabilidad de todos los colaboradores, que tengan acceso a la información de la Municipalidad de Montes de Oro, cumplir con todas las políticas y procedimientos definidos frente a la protección de la información, las cuales le han sido suministrados para la labor designada y así mismo usar de manera segura los documentos de información que le fueran asignados. Estos colaboradores deben estar autorizados por el responsable, quien será el gestor del control y vigilancia del uso adecuado de los activos de información. Los colaboradores deben aceptar por escrito los términos y condiciones de uso de la información, así como el cumplimiento estricto de las políticas de seguridad de la información de la entidad antes de su acceso a los mismos.

5.1.2 Cifrado e Información Confidencial

A. Descripción General

Dado a la naturaleza de la información que se maneja en la Municipalidad de Montes de Oro, se debe considerar la sensibilidad de los datos que residen en los sistemas de información para el debido control y acceso. Pérdida o mal uso de esta información puede resultar en una variedad de daños, tales como pérdida de confidencialidad e incumplimiento de regulaciones y leyes aplicables a la entidad.

B. Propósito

Establecer normas para el uso de algoritmos de encriptación y servicios de protección de información a utilizar en la Municipalidad de Montes de Oro y para el uso, protección y vida útil de las claves criptográficas durante toda su vida útil en cumplimiento con todos los acuerdos, la legislación y las normativas pertinentes.

C. Alcance

Esta política se aplica al uso de algoritmos de cifrado como herramientas de control, protección de la confidencialidad, autenticidad o integridad de la información, así como la debida documentación y resguardo de estos.

Debe ser cumplida por todos los usuarios en la Municipalidad de Montes de Oro, incluyendo las empresas que presten servicios a la entidad.

D. Aplicación

1. Generalidades

Se debe cifrar toda la información sensible, clasificada como confidencial, que pudiese quedar expuesta a usuarios no autorizados, en relación con su privacidad e integridad.

Se deben utilizar controles criptográficos para la protección de la confidencialidad, el cumplimiento del principio de la no repudiación y el control de integridad de la información en los siguientes casos:

- Protección de claves de acceso a sistemas, documento electrónico, datos y servicios.
- Transmisión de información clasificada fuera del ámbito del servicio.
- Resguardo de información cuando así surja de la evaluación de riesgos realizada por el propietario de la información y el encargado de seguridad de la información.

2. Acerca de la confidencialidad

Se definen los algoritmos de cifrado que podrán utilizarse al interior de la Municipalidad de Montes de Oro, como una aplicación directa o como parte de la configuración de otros productos de seguridad comerciales, tomando en cuenta el tipo y la calidad del algoritmo de cifrado utilizado y la longitud de las claves criptográficas. Sólo se utilizan algoritmos de cifrado definidos en estándares internacionales.

3. Acerca de la integridad/autenticidad

Para verificar la autenticidad o integridad de la información almacenada o transmitida sensible o crítica, la Municipalidad de Montes de Oro utiliza como mecanismo criptográfico la firma digital bajada en certificados digitales. En el caso de documentos electrónicos, estos son de carácter de firma electrónica avanzada.

4. Acerca de la Autenticación

Se utilizan técnicas criptográficas para autenticar a los usuarios o entidades externas que requieren hacer uso de los sistemas de información de la Municipalidad de Montes de Oro. Los funcionarios deben usar el sistema autorizado por la Municipalidad de Montes de Oro para efecto de autenticación.

El encargado de seguridad debe ser informado inmediatamente en caso de que se reciba cualquier comunicado por cualquier medio de comunicación de parte de una autoridad de protección de datos u otro ente regulador.

5. Registro y cancelación de registro de usuarios

Este mecanismo de autentificación (claves de acceso, dispositivo u otro) debe ser asignado individualmente, quedando prohibido el uso de un nombre de usuario ajeno o facilitar el usuario y su contraseña personal a un tercero.

El Departamento de Gestión de Personas es responsable de notificar por escrito al Departamento de Informática y Telecomunicaciones sobre el ingreso, salida o traslado de un usuario. Esto con el fin de que se creen, inhabiliten, modifiquen o eliminen privilegios de acceso a las diferentes plataformas, documentación, dominios y dispositivos correspondientes.

6. Uso de la información de autenticación secreta

Todos los funcionarios que presten servicios a la Municipalidad de Montes de Oro tienen la obligación de cumplir con las siguientes directrices:

- Mantener la información de autenticación secreta como confidencial, asegurándose de que no se divulgue a ninguna otra parte, incluidas las personas con autoridad.
- Evitar mantener un registro (es decir, en papel, archivo de software o en un dispositivo de mano) de la información de autenticación secreta.
- Cambiar la información de autenticación secreta cuando exista alguna sospecha de que pudiera haber sido vulnerada o conocida por terceros.
- No se debe compartir la información de autenticación secreta de usuario de una persona.

7. Contraseñas en Dispositivos de Red

Todos los dispositivos de red (routers, firewalls, switches) deben tener contraseñas únicas u otro mecanismo de control de acceso.

Si un dispositivo no posee contraseña de acceso, se debe impedir su administración remota, permitiendo la intervención sólo al personal autorizado y en forma directa (conexión local).

8. Contraseña por Omisión y recordatorios de contraseña

Toda contraseña por omisión provista por el fabricante de cualquier sistema debe ser reemplazada inmediatamente.

Queda absolutamente prohibido anotar las contraseñas de acceso en lugares públicos.

Cualquier contraseña encontrada en estos medios debe ser informada al encargado del Departamento de informática y tratada como un incidente.

9. Acceso a Información Sensible

En el caso del control de acceso a información, se deben utilizar contraseñas robustas seguras o cifradas.

La contraseña nunca debe ser compartida o revelada; hacer esto responsabiliza al usuario que prestó la contraseña de acceso y a todas las acciones que se realicen de la misma.

Frente a la evidencia de un compromiso del sistema por uso indebido de cuentas con privilegios, todas las contraseñas de cuentas con privilegios del sistema deben ser reemplazadas y se debe registrar como un incidente de seguridad.

5.1.3 Gestión de cuentas

A. Descripción General

La Municipalidad de Montes de Oro considera indispensable regular la creación, suspensión, reactivación, eliminación de usuarios de red y correo electrónico.

B. Propósito

El objetivo de la política es regular la creación, suspensión, reactivación, eliminación de usuarios de red y de correo electrónico, para lo cual, se emiten los siguientes lineamientos que son de cumplimiento obligatorio para todo el personal de la Municipalidad de Montes de Oro.

C. Alcance

Es necesario que todos los usuarios estén enterados y conscientes de los compromisos, normas y reglamentos que se dictan para la creación de este tipo de cuentas, tomando todas las medidas que correspondan, para que estas se respeten y se cumplan, ya que las cuentas de red y correo electrónico dan acceso a gran variedad de recursos informáticos que deben manejarse con cautela

El uso de la red y recursos de información, están disponible para fortalecer el flujo de información interna, la investigación y el apoyo a las diferentes tareas encomendadas para mejoramiento de nuestras labores. Todos los usuarios de la red están sujetos a esta política y a los términos de esta. El uso inapropiado de la red podría ser sancionado con la eliminación del acceso a estos recursos y puede conllevar a la aplicación de las sanciones disciplinarias respectivas, además de las consecuencias de índole legal que sean aplicables.

D. Aplicación

1. Solicitud de creación de usuarios de red y correo electrónico.

Para la creación de usuarios nuevos de red y de correo electrónico, se deben seguir los siguientes pasos:

1. Debe existir una solicitud expresa por parte del Departamento de Recursos Humanos para usuarios en el Departamento de Tecnologías de Información, solicitando la creación de los accesos. Esta solicitud debe incluir al menos lo siguiente:

- Nombre completo de la persona
- Número de Identificación: Cédula Nacional, Cédula de Residencia o Pasaporte.
- Indicar si es un funcionario interino, en propiedad o un pasante.
- En caso de ser un funcionario en situación interina o pasante, se debe indicar una fecha de finalización de las labores, con el fin de limitar el acceso a los recursos informáticos hasta la fecha que se indique.
- Departamento al que pertenece el nuevo funcionario.

2. Una vez recibida la solicitud en el Departamento de Tecnologías de Información, se procederá a realizar la creación del usuario de red y del correo electrónico. El usuario de red será creado a partir del número de identificación brindado en la solicitud. También, se creará una cuenta de correo electrónico que consta de:

a. Una dirección electrónica con la forma usuario@municipalidadmontesoro.go.cr.

b. Una palabra clave o contraseña para acceder de manera privada a la cuenta.

c. La posibilidad de enviar y recibir mensajes en la Intranet y hacia Internet utilizando la dirección electrónica asignada.

3. Dadas las limitaciones de cuentas con que cuenta el Departamento de Tecnologías de Información, sólo se crearán cuentas de correo para funcionarios interinos o en propiedad, limitando el acceso a estas a las personas que realicen pasantías en la Institución.

4. Todo usuario para tener acceso a los recursos de red y al correo electrónico, deberá quedar registrado en la Base de Datos de Usuarios de red del Departamento de Tecnologías de Información.

5. Una vez creados los accesos correspondientes, el Departamento de Tecnologías de Información se encargará de notificar la cuenta y clave de acceso, al responsable de la solicitud para que la retire en las oficinas del Departamento de Recursos Humanos. Las claves creadas por el Departamento son temporales, por lo que se deben cambiar en el primer ingreso del usuario. La nueva clave debe cumplir con las siguientes características:

1. Tamaño mínimo de 8 (ocho) caracteres.
2. Utilizar letras mayúsculas (de la “A” a la “Z”), minúsculas (de la “a” a la “z”), números (del “0” al “9”) y preferiblemente caracteres especiales como $, #, &, * (asterisco) y (punto).
3. No se permitirá claves en blanco.
4. Evitar el uso de su nombre, sus apellidos, nombres de personas, animales, iniciales familiares, cédulas.
5. No usar secuencias básicas de caracteres que cambian parcialmente con base en la fecha u otro factor fácilmente predecible.

6. Se recomienda realizar un cambio de contraseña por lo menos una vez cada 30 días naturales.

6. Es importante aclarar que la misma contraseña del usuario de red es la que se utiliza para acceder al correo electrónico

2. Solicitud de suspensión temporal de usuarios de red y correo electrónico.

Para la suspensión temporal de usuarios de red y de correo electrónico, se deben seguir los siguientes pasos:

1. Se puede dar por motivos de seguridad informática ante el conocimiento previo del Departamento de Tecnologías de Información respecto a la separación del cargo, de algún funcionario de la institución, ya sea este por motivos de despido, suspensión temporal, permiso sin goce se salario, u alguna otra situación contemplada por la gestión de Recursos Humanos. También puede darse una suspensión temporal de los accesos si se detecta desde el Departamento de Tecnologías de Información, algún acceso indebido u otro evento que pueda afectar la integridad y seguridad de las cuentas del funcionario. O bien, mediante la tramitación inmediata de una solicitud expresa por parte del Departamento de Recursos Humanos, por medio de un correo electrónico para el Departamento de Tecnologías de Información, solicitando la suspensión de los accesos. Esta solicitud debe incluir al menos lo siguiente:

- Nombre completo de la persona
- Número de Identificación: Cédula Nacional, Cédula de Residencia o Pasaporte
- Indicar si es un funcionario interino o en propiedad.
- Departamento al que pertenece el nuevo funcionario.

- Fecha a partir de la cual se hace una suspensión temporal de los accesos.

2. Seguidamente se procederá a realizar la suspensión del usuario de red y del correo electrónico, manteniéndose en dicho estado hasta que no exista una solicitud de reactivación o eliminación de la cuenta en definitiva por parte de Recursos Humanos.

3. Solicitud de reactivación de una cuenta de usuarios de red y correo electrónico suspendida.

Para la reactivación de usuarios de red y de correo electrónico, se deben seguir los siguientes pasos:

1. Debe existir una solicitud expresa por parte del Departamento de Recursos Humanos, por medio de un correo electrónico para el Departamento de Tecnologías de Información, solicitando la reactivación de los accesos. Esta solicitud debe incluir al menos lo siguiente:

- Nombre completo de la persona.
- Número de Identificación: Cédula Nacional, Cédula de Residencia o Pasaporte.
- Indicar si es un funcionario interino o en propiedad.
- Departamento al que pertenece el nuevo funcionario.
- Fecha a partir de la cual se debe hacer la reactivación de los accesos.

2. Una vez recibida la solicitud en el Departamento de Tecnologías de Información, se procederá a realizar la reactivación del usuario de red y del correo electrónico, a partir de la fecha que se indique en la solicitud.

4. Solicitud de eliminación de una cuenta de usuarios de red y correo electrónico suspendida.

Para la eliminación de usuarios de red y de correo electrónico, se deben seguir los siguientes pasos:

1. Debe existir una solicitud expresa por parte del Departamento de Recursos Humanos, por medio de un correo electrónico para el Departamento de Tecnologías de Información, solicitando la eliminación de los accesos. Esta solicitud debe incluir al menos lo siguiente:

- Nombre completo de la persona.
- Número de Identificación: Cédula Nacional, Cédula de Residencia o Pasaporte.
- Indicar si es un funcionario interino o en propiedad.
- Departamento al que pertenece el nuevo funcionario.
- Fecha a partir de la cual se debe hacer la reactivación de los accesos.

2. Una vez eliminados los accesos, el usuario tendrá 30 días naturales (1 mes calendario), para que pueda solicitar un respaldo de su correo electrónico, esto antes de que su cuenta sea eliminada por completo del sistema de correo electrónico institucional.

5. Responsabilidades.

1. Cada usuario y funcionario es responsable de los mecanismos de control de acceso a la red, que les sean proporcionados; esto es, de su “Usuario” (número de cédula del funcionario) y contraseña necesarios para acceder a la red interna de información y a la infraestructura tecnológica de la Municipalidad de Montes de Oro, por lo que se deberá mantener de forma confidencial.

2. Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por el Departamento de Tecnologías de Información antes de poder usar la infraestructura tecnológica de la Municipalidad de Montes de Oro.

3. Los usuarios no deben proporcionar información a personas externas, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica de la Municipalidad de Montes de Oro.

4. Cada usuario que acceda a la infraestructura tecnológica de la Municipalidad de Montes de Oro, debe contar con un identificador de usuario (número de cédula) único y personalizado. Por lo cual, no está permitido el uso de un mismo identificador por varios usuarios.

5. Los usuarios y funcionarios son responsables de todas las actividades realizadas con su identificador de usuario (ID). Los usuarios no deben divulgar ni permitir que otros utilicen sus identificadores de usuario, ni tampoco utilizar el ID de otros usuarios.

6. La asignación de contraseñas debe ser realizada de forma individual, y por tanto no debe ser compartida. Hacer esto responsabiliza al usuario que prestó su contraseña de todas las acciones que se realicen con su cuenta de correo.

7. Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá apersonarse al Departamento de Tecnologías de Información para que se le proporcione una nueva contraseña.

8. Las contraseñas no deben registrarse o anotarse en un lugar donde personas no autorizadas puedan descubrirlos, tampoco se deben almacenar en ningún programa o sistema que proporcione esta facilidad y que pueda ser utilizado por terceras personas.

9. Por seguridad de la información nunca se debe utilizar opciones de los sistemas para “recordar las contraseñas”, esto por cuanto el acceso queda directo y cualquier persona que ingrese a ese equipo podría hacer uso de esa cuenta de correo

10. Todo usuario que tenga la sospecha de que su contraseña es conocida por otra persona, deberá cambiarlo inmediatamente.

11. No utilice comandos o programas o el envío de mensajes de cualquier tipo con el propósito de interferir o deshabilitar una sesión de usuario a través de cualquier medio, local o remoto (Internet o Intranet).

6. Uso y administración del correo electrónico.

A. La cuenta de correo electrónico

Se entiende por cuenta de correo electrónico la asignación por parte de la Municipalidad de Montes de Oro:

- Una dirección electrónica con la forma usuario@municipalidadmontesoro.go.cr.
- Un buzón (espacio en disco) para almacenar los mensajes.
- Una palabra clave o contraseña para acceder de manera privada a la cuenta.
- La posibilidad de enviar y recibir mensajes a buzones de otras plataformas de correo, dentro y fuera del país.
- Formato de las cuentas de Usuario: Con el fin de garantizar que la identificación del usuario en la dirección de correo sea única, se seguirán las

siguientes reglas para construir cada identificación: se formará con la primera letra del nombre del usuario y el primer apellido (sin tildes, mayúsculas, ni signos propios de algunos idiomas). En caso de presentarse coincidencias en la identificación de dos usuarios se resolverá de acuerdo con el orden de procesamiento: el primer usuario recibirá la identificación antes mencionada, al segundo usuario se le asignará la primera letra del nombre del usuario, el primer apellido, y la primera letra del segundo apellido.

- La primera vez que un usuario reciba su cuenta de correo, deberá cambiar su clave.
- Para reportar problemas o realizar cualquier solicitud que tenga relación con cuentas de correo o el servicio de correo electrónico en general, se debe hacer la correspondiente solicitud de servicio en la Intranet.
- Es responsabilidad de cada usuario tener copias de respaldo de los mensajes de sus carpetas de correo y de su agenda de direcciones electrónicas.

B. Buen uso del correo electrónico.

En la Municipalidad de Montes de Oro deberá utilizarse para trabajar solamente el correo oficial institucional, excluyendo servicios comerciales como Hotmail, Yahoo, Gmail, entre otros.

Es responsabilidad de los usuarios:

- Usar su cuenta con fines laborales de acuerdo con las funciones propias del puesto que le ha sido asignado en la Municipalidad de Montes de Oro.
- Se debe utilizar el logo institucional

C. Seguridad de la información.

Tome en cuenta las siguientes medidas de Seguridad:

- Antes de responder un mensaje, asegúrese que vaya dirigido a usted.
- Cerciore antes de contestar un mensaje, de que conoce la dirección.
- No envíe ni conteste cadenas de correo o cualquier otro esquema de "pirámide" de mensajes.
- No use su cuenta para fines comerciales.
- Analice y verifique cada correo antes de abrirlo, aun cuando cree conocer la cuenta que le envío el mensaje, por ningún motivo se deben abrir correos malintencionados tipo “phishing”.
- Debe borrar de inmediato cualquier mensaje que sea sospechoso, para no exponer el correo Institucional a un posible ataque o hurto de información.
- Nunca proporcione información confidencial por correo, ni facilite usuarios o contraseñas, de ningún tipo.
- Los usuarios no deben leer correo ajeno ni generar o enviar correos electrónicos a nombre de otra persona sin autorización o suplantándola.
- Nunca se inscriba a listas de correos que no conozca.
- La Municipalidad de Montes de Oro se reserva el derecho de monitorear mediante el Departamento de Tecnologías de Información las cuentas que presenten un comportamiento sospechoso.
- Con el fin de agilizar el envío de información, no se podrán enviar mensajes masivos, a menos que sea un asunto oficial.
- No se debe falsificar, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.
- No se debe interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.
- No envíe mensajes a gente que no conoce, a menos que exista una razón de peso de por medio
- No envíe mensajes ofensivos, abusivos, etc.

5.1.4 Manejo de Información.

A. Descripción General

Describir las actividades que adquieren cada uno de los colaboradores de la Municipalidad de Montes de Oro con relación al manejo de la información.

B. Propósito

Tiene como propósito describir las actividades, procedimientos y responsabilidades de los colaboradores de Municipalidad de Montes de Oro con relación al manejo de la información personal de sus usuarios, así como todas las medidas de seguridad que se adoptan para la protección de la información y las normas que rigen las diferentes actividades aquí comprendidas.

C. Alcance

Comprende todos los procesos de la empresa que captan, manipulan y comparten información hasta su disposición final.

D. Aplicación

A. Identificación Y Autorización.

- Cada uno de los colaboradores de la Municipalidad de Montes de Oro se identifica en el Sistema de la Institución con un usuario y contraseña.

- El cargo que tenga cada empleado, definirá el nivel de permisos que tiene para ingresar, consultar y actualizar información.
- Para el Servidor de Archivos, se definen los documentos que pueden ser de acceso interno y los que requieren un permiso exclusivo que son almacenados en carpetas privadas, de lectura y de edición.

B. Control de Acceso.

- Bajo los mecanismos de identificación y autorización establecidos se evitará que un usuario pueda acceder a recursos a los cuales no tiene autorización.
- Los niveles de acceso a las bases de datos y al Servidor de Archivos se definen de acuerdo al perfil del cargo, en caso de que se cree un cargo nuevo se debe establecer primero el perfil para identificar el nivel de seguridad y acceso que se necesita para el ingreso.
- Cuando un empleado se retira de la Municipalidad de Montes de Oro, el Departamento de Recursos Humanos debe notificar al Departamento de Tecnologías de Información para que desactive el usuario en los diferentes sistemas.
- En caso de requerir acceso especial y el cargo no lo posea, el empleado lo solicita al Departamento de Tecnologías de Información quien analiza la petición y de ser procedente asignará los permisos.

C. Registro de Acceso.

Siempre que se realice una modificación a los datos contenidos en el Sistema de la Institución se registra identificando: la información modificada, hora y fecha de modificación, usuario que modificó y desde que equipo se realiza la modificación.

Los datos del registro de modificación, anulación y eliminación se conservan indefinidamente y solo el personal autorizado, tiene acceso en modo de consulta al módulo de auditoría del Sistema de la Institución.

Para el caso de la información almacenada físicamente en el Archivo central, se hace la solicitud de acceso a la documentación requerida al Departamento de Tecnologías de Información de acuerdo al protocolo de acceso que se tenga establecido.

D. Acceso a Datos a Través de Redes de Comunicaciones.

Las bases de datos de la Municipalidad de Montes de Oro, solo serán accesibles estando conectados a la red interna, además, tanto el Servidor de Archivos como el Sistema de la Institución tienen medidas de seguridad que limitan el acceso a la información y el nivel de permisos que se tenga para la modificación de la misma.

Los accesos al Sistema de la Institución serán controlados a través de usuario y clave personal que posee cada uno de los empleados de la Municipalidad de Montes de Oro, los cuales se gestionan de acuerdo al nivel de permiso que se requiera según el perfil del cargo que ocupa el colaborador y le dan acceso

restringido a tipo de información necesaria para el desarrollo de sus actividades laborales.

El Servidor de Archivos cuenta con acceso restringido a la información de acuerdo a lo que disponga el colaborador encargado de la información, contando con archivos privados de cada área en particular e información que se permite compartir, alguna con objetivos de edición y otra con objetivos de solo lectura

E. Copias de Respaldo y Recuperación.

La creación y actualización de datos se lleva en los Sistemas de la Institución, los cuales se almacenan directamente en servidores, estos están configurados para realizar copias de seguridad diarias, se transfieren al finalizar el día a un disco duro externo y se clasifican en tres grupos:

- Abuelo: contiene los respaldos mensuales por año y el del último mes del año inmediatamente anterior.
- Padre: contiene los respaldos semanales (viernes de cada semana).
- Hijo: contiene el respaldo realizado día a día de lunes a viernes.

Los procedimientos establecidos para las copias de respaldo y para su recuperación garantizarán su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. El responsable de la información verificará semestralmente los procedimientos de copias de respaldo y recuperación de los datos. Las pruebas anteriores a la implantación o modificación de sistemas de información se realizarán con datos reales previa copia de seguridad, y garantizando el nivel correspondiente al tratamiento realizado.

F. Información y Obligaciones del Personal.

Para asegurar que todas las personas conocen las normas de seguridad que afectan al desarrollo de sus funciones, serán informadas de acuerdo con el siguiente procedimiento:

- En el momento de realizar la inducción y entrenamiento, el encargado de realizarla debe socializar con los diferentes colaboradores bajo su cargo las medidas que afectan en el desarrollo de las actividades de su ejercicio laboral.
- A través del medio interno de comunicación, se recordará periódicamente la existencia de las normas de seguridad y las consecuencias de su incumplimiento.
- Una vez al año, el responsable de Tecnologías de Información realiza una reunión con todo el personal para socialización y refuerzo del conocimiento de las medidas de seguridad de manejo de la información.
-

G. Funciones y Obligaciones del Personal.

Constituye una obligación del personal notificar al Departamento de Tecnologías de Información las incidencias de seguridad de las que tengan conocimiento respecto a los recursos protegidos.

Todas las personas deberán guardar confidencialidad sobre los datos personales que conozcan en el desarrollo de su trabajo, compromiso pactado en el contrato laboral de trabajo y/o de prestación de servicios.

Funciones y obligaciones de los colaboradores de la Municipalidad de Montes de Oro:

- Velar por el cumplimiento de las medidas de seguridad de la información al interior de la empresa, gestionar el conocimiento de dichas medidas y las consecuencias del incumplimiento de las mismas.
- Gestionar y verificar que los cargos asociados a su área posean los permisos para acceder a la información contenida en las bases de datos necesarias para el desempeño de sus actividades laborales.
- Velar por la adecuada disposición y el mantenimiento integral de la información, por parte del personal de la organización que requiera los documentos.
- Conocer y respetar las normas y procedimientos para el adecuado uso de la información tanto física como virtual de los usuarios de la Municipalidad de Montes de Oro.

El personal que realice trabajos que no impliquen el tratamiento de datos personales tendrán limitado el acceso a estos datos, a los documentos que contengan o a los recursos del Sistema de la Institución.

Cuando se trate de personal ajeno a Institución, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales.

En caso que por la naturaleza de las actividades desarrolladas por el contratista y necesite acceder a información personal, en el contrato se expresa la obligación de confidencialidad respecto a aquellos datos que hubiera podido conocer durante la prestación del servicio.

5.1.5 Gestión del cambio

A. Descripción General

Todo cambio sobre un activo y/o elemento de configuración en los ambientes de producción debe realizarse mediante una solicitud de cambio, es decir que debe registrarse y gestionarse con el Departamento de Tecnologías de Información.

Todo cambio debe tener un técnico responsable asignado, quien desempeña el rol de gestor del cambio.

B. Propósito

El objetivo es definir y establecer directrices que le permitan a la universidad evaluar los cambios internos y externos sobre el Sistema de la Institución, minimizando la aparición de nuevos riesgos en el entorno laboral a medida que suceden los cambios.

C. Alcance

Se debe o puede incluir cambios en todos los servicios, arquitecturas, procesos, herramientas, métricas y documentación para la gestión de cambios en Infraestructura y Operaciones de TI.

D. Aplicación

1. Identificar el tipo de cambio.

Se debe identificar, describir, clasificar y justificar el cambio de este procedimiento.

2.Analizar el impacto del cambio al sistema de gestión de seguridad.

Identificar y evaluar el impacto y los riesgos a los que se enfrenta el proceso con la implementación del cambio previsto, teniendo en cuenta los efectos o consecuencias del cambio y establecer los controles para minimizar riesgos e impactos.

3.Registrar las actividades del plan de gestión de cambios.

Luego de identificados los posibles impactos y riesgos, se realiza el plan de intervención o plan de gestión del cambio que debe incluir: actividad, responsable, comunicación, fecha seguimiento, estado del cambio (en ejecución o cerrado) si fue eficaz: (si /no)

4.Comunicar el plan de gestión de cambios a los interesados.

Comunicar el plan de gestión del cambio, para que conjuntamente trabajen con el responsable del proceso.

5.Implementar el plan de gestión de cambios.

Los responsables deben informar sobre las novedades que se generen en el proceso de implementación de acciones con el fin de tomar decisiones respecto a dichas novedades para que los riesgos derivados del cambio no se materialicen o los impactos se minimicen

Cada vez que se realice un cambio en el Sistema de la Institución, se tendrá en cuenta la identificación de peligros, valoración de riesgos e identificación de aspectos e impactos.

Cuando se trate de cambios en la documentación, deberán ser difundidos según la matriz de comunicaciones de la Institución. Así mismo, cuando se trate de cambios en el perfil de cargo, se deberá informar a cada colaborador, con el fin de garantizar su entendimiento.

Cuando se trate de activos, se establecerá un procedimiento para la operación de la misma el cual estará orientado a un manual de operaciones o, además se establecerá los controles en la matriz de peligros; se debe asegurar que el colaborador que vaya a utilizar el activo entienda la forma de operación y los riesgos y los controles y si es posible tratar que el trabajador reciba el entrenamiento directamente del fabricante o el distribuidor del activo.

5.1.6 Gestión de incidentes

A. Descripción General

Contar con una política de gestión de incidentes es clave para garantizar la supervivencia de la empresa ante los efectos negativos causados por un ataque de ciberseguridad. Es fundamental diseñar un plan que determine el alcance de las acciones a realizar en cuanto se detecte el incidente y la respuesta al mismo para mitigar al máximo su impacto.

B. Propósito

Gestionar adecuadamente todos los incidentes de seguridad de la información reportados en la Municipalidad de Montes de Oro dando cumplimiento a los procedimientos establecidos.

C. Alcance

Esta política aplica para todos los colaboradores de la Municipalidad de Montes de Oro que detecten un evento o incidente de seguridad de la información el cual deben reportar.

D. Aplicación

A. Responsabilidades y procedimientos.

Para establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información hay que tener en cuenta lo siguiente:

- Establecer las responsabilidades en la gestión de incidentes de seguridad digital dentro del MEN.
- Definir el procedimiento de atención de incidentes de seguridad de la información del MEN.
- Dar un tratamiento adecuado a todos los incidentes de seguridad de la información reportados en el MEN.
- Realizar sensibilización a todos los colaboradores y terceros sobre incidentes de seguridad de la información.

B. Reporte de eventos de seguridad de la información.

- Informar sobre los eventos de seguridad de la información a través de los canales de gestión apropiados, tan pronto como sea posible.
- Reportar de forma inmediata de acuerdo con el procedimiento previsto los eventos, incidentes o debilidades en cuanto a la seguridad de la información que identifiquen o se presenten.

C. Evaluación de eventos de seguridad de la información.

- Evaluar los eventos de seguridad de la información y decidir si se van a clasificar.
- Evaluar cada evento o incidente de seguridad de la información presentado en la Municipalidad de Montes de Oro, con el fin de poder determinar clasificación y priorización.
- Registrar los resultados de la evaluación y la decisión para referencia y verificación futuras.

D. Respuesta a incidentes de seguridad de la información.

Responder a los incidentes de seguridad de la información que se presenten en la Municipalidad de Montes de Oro.

La respuesta debe incluir lo siguiente:

- Recolectar evidencia lo más pronto posible después de que ocurra el incidente.
- Llevar a cabo análisis forense de seguridad de la información, según se requiera.
- Llevar el asunto a una instancia superior, según se requiera.
- Asegurarse de que todas las actividades de respuesta involucradas se registren adecuadamente para análisis posterior.
- Tratar las debilidades de seguridad de información que se encontraron que causan o contribuyen al incidente.
- Una vez que el incidente se haya tratado lo suficiente, cerrarlo formalmente y hacer un registro de esto.

E. Aprendizaje obtenido de los incidentes de seguridad de la información.

- Usar el conocimiento adquirido al analizar y resolver incidentes de seguridad de la información para reducir la posibilidad o el impacto de incidentes futuros.
- Documentar todos los incidentes de seguridad de la información reportados en la Municipalidad de Montes de Oro.
- Llevar una bitácora de los incidentes de seguridad de la información reportados y atendidos en la Municipalidad de Montes de Oro.

F. Recolección de evidencia.

- Definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
- Desarrollar y seguir procedimientos internos cuando se trata con evidencia para propósitos de acciones legales y disciplinarias en la Municipalidad de Montes de Oro.

5.1.7 Control de activos de información

A. Descripción General

La Municipalidad de Montes de Oro comprende la importancia de una adecuada gestión de los activos, por lo cual tener un inventario y conocer la responsabilidad de los activos de información es parte esencial del sistema de gestión de Seguridad de la Información de la entidad, dado que a través de éste se conoce cuántos activos tiene la entidad, sus propietarios y los responsables de los mismos.

B. Propósito

Definir las políticas para la gestión de los activos de la institución que incluye el inventario y la responsabilidad sobre los activos de información.

C. Alcance

Aplica para todos los colaboradores de la Municipalidad de Montes de Oro que tenga acceso a los recursos y activos de información durante su ciclo de vida (creación, distribución, transmisión, almacenamiento, eliminación), y a los activos de información en todas sus formas (digital, impresa, escrita, y verbal).

D. Aplicación

A. Inventario de Activos.

1. Inventario de Activos.

Se deben identificar los activos asociados con la información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.

2. Propiedad de los Activos.

Los activos de información que hacen parte del inventario deben tener un propietario o responsable, de acuerdo con la asignación de activos fijos en el caso del hardware y de la información de acuerdo con el rol desempeñado en la entidad.

3. Encargado de inventarios de activos de información.

Responsable encargado de generar, mantener y actualizar el inventario de los activos de la entidad, así como la asignación indicando los responsables de la custodia de dichos activos.

4. Personal de la Municipalidad de Montes de Oro.

Responsable encargado de garantizar la integridad, confidencialidad y disponibilidad del inventario de activos que este bajo su custodia.

5. Uso Aceptable de los Activos.

Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.

6. Devolución de los Activos.

Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.

7. Etiquetado de Activos.

Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la entidad.

8. Eliminación de Activos.

La eliminación o destrucción de los activos de información, sean estos documentos en papel, bienes muebles (equipos, computadores, notebook, u otros similares), deberá efectuarse de acuerdo con la normatividad vigente.

5.1.8 Detección de intrusión

A. Descripción General

Un Sistema de Detección de Intrusos es un programa utilizado para analizar la detección de supuestos intrusos en la red o un computador, basado en sensores virtuales, permiten monitorear el tráfico de la red, permitiendo así evitar posibles ataques.

B. Propósito

Es un proceso de auditoría de la información del sistema de la red o de un computador, logrando a través de una configuración y de una base de datos prevenir y detectar posibles ataques de intrusos.

C. Alcance

Esta política aplica para todos los colaboradores de la Municipalidad de Montes de Oro que detecten un evento o incidente de seguridad de la información.

D. Aplicación

El proceso de detección de intrusos, se lo define de la siguiente manera:

- Una base de datos con una recopilación de ataques anteriores.
- Un sistema actual debidamente configurado.

- Estado actual, referente en términos de comunicación y procesos.

Además, el Sistema de Detección de Intrusos posee diferentes tipos los cuales se especificarán a continuación:

- Sistema de Detección de Intrusos basados en Host, estos solo procesan determinadas actividades de los usuarios o computadoras.
- Sistema de Detección de Intrusos basados en Red, monitorean generalmente algún punto de la red, en busca de intrusos. Bien ubicados en la red, pueden ser una alternativa excelente para la prevención de los intrusos y un bajo impacto en la red al abarcar grandes redes.
- Sistema de Detección de Intrusos basados en Log, revisa los archivos de Logs en busca de posibles intrusos, se caracteriza por su precisión y completitud.

Todos estos Sistemas de Detección serán usados por el Departamento de Tecnologías de Información y el mismo departamento tomara las medidas necesarias para controlar la intrusión.

5.1.9 Acceso a la red

A. Descripción General

Diseñar una política para garantizar que la red informática esté protegida de cualquier acto o proceso que pueda violar su seguridad.

B. Propósito

Fortalecer la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte de la Municipalidad de Montes de Oro.

C. Alcance

Esta política aplica para todas las redes, los servicios de red y los controles utilizados para proteger la información en la transferencia de información de la Municipalidad de Montes de Oro.

D. Aplicación

A. Controles de Redes.

- Gestionar y controlar las redes para proteger la información en sistemas y aplicaciones.
- Establecer los controles lógicos para el acceso a los diferentes recursos informáticos, con el fin de mantener los niveles de seguridad apropiados.
- Proporcionar a los colaboradores y terceros todos los recursos tecnológicos de conectividad necesarios para que puedan desempeñar las funciones y actividades laborales.
- Monitorear la funcionalidad de las redes a través del uso de analizadores de red.
- No es permitido conectar a las estaciones de trabajo o a los puntos de acceso de la red corporativa, elementos de red (tales como switches, enrutadores, módems, etc.) que no sean autorizados por el Departamento de Tecnologías de Información.

B. Seguridad de los servicios de red.

- Dar el acceso a internet exclusivamente a través de la red establecida para ello, es decir, por medio del sistema de seguridad con Firewall incorporado en la misma.
- Utilizar el acceso a la red, Internet, exclusivamente para el desarrollo de sus actividades propias de las funciones desempeñadas en la Municipalidad de Montes de Oro.
- El acceso de los colaboradores a la red debe realizarse a través de la red inalámbrica definida como (MuniMonOro) o mediante la red cableada.
- Conectarse única y exclusivamente a la red inalámbrica (InviMonOro) de la Municipalidad de Montes de Oro a internet sin la necesidad de algún tipo de cableado. La red inalámbrica de invitados le permitirá utilizar los servicios de internet, en las zonas de cobertura de la Municipalidad de Montes de Oro.
- Los usuarios que accedan a través de la red invitados no tendrán acceso a los servicios, sistemas de información, etc., de la Municipalidad de Montes de Oro ni a ningún recurso de uso privado.

C. Separación en las redes.

- Establecer un esquema de segregación de redes, con el fin de controlar el acceso a los diferentes segmentos de red y buscar que se preserve la confidencialidad, integridad y disponibilidad de la información de la Municipalidad de Montes de Oro.

- Establecer parámetros técnicos para la conexión segura de la red con los servicios de red.
- Establecer mecanismos de autenticación seguros para el acceso a la red.
- Separar las redes inalámbricas públicas de las redes internas, para preservar los principios de la seguridad de la información.

5.1.10 Acceso físico

A. Descripción General

Lo definido en la presente política aplica para el control de acceso físico a las áreas seguras dentro de las cuales se encuentran el centro de datos, centros de cableado, áreas de tesorería, archivo, áreas de recepción y entrega de correspondencia y controles de acceso adecuados para la protección de la información de la Municipalidad de Montes de Oro.

B. Propósito

Prevenir el acceso físico no autorizado, el daño y la interferencia a la información a las instalaciones de procesamiento de información de la Municipalidad de Montes de Oro.

C. Alcance

Aplica para todos los colaboradores de la Municipalidad de Montes de Oro que tengan acceso a diferentes áreas de la institución, esto con el fin de controlar el acceso físico a las áreas donde se encuentras los centros de datos.

D. Aplicación

A. Perímetro de seguridad física.

- El perímetro de seguridad de las instalaciones de la Municipalidad de Montes de Oro o de las áreas seguras debe ser físicamente sólido (no deben existir aberturas en el perímetro o áreas donde pueda producirse fácilmente una irrupción). Las paredes externas del área deben ser de construcción sólida y todas las puertas que comunican con el exterior deben ser adecuadamente protegidas contra accesos no autorizados, por ejemplo, mediante mecanismos de control, vallas, alarmas, cerraduras, etc.
- Verificar que las puertas y ventanas de las áreas seguras estén cerradas con llave cuando no hay supervisión o están desocupadas.
- El perímetro de seguridad de las áreas seguras debe contar con vigilancia mediante CCTV, contar con sistemas de control de acceso y debe ser monitoreado por el personal de seguridad de la institución.
- Todas las puertas de emergencia de un perímetro de áreas seguras deben tener alarma.

B. Controles de acceso físico.

- Todos los puntos de acceso a las instalaciones físicas deberán tener un área de recepción con vigilancia u otro medio para controlar el acceso físico a las instalaciones y debe estar documentado.

- El personal de seguridad debe establecer mecanismos para inspeccionar y examinar los bolsos, cajas, etc. de los colaboradores o visitantes que ingresen y salen de las instalaciones de la Municipalidad de Montes de Oro.
- Registrar en una bitácora o sistema de información el ingreso y retiro de todo equipo de cómputo, servidores, equipos activos de red o cualquier equipo diferente a smartphone; en caso de que estos equipos sean propiedad del Ministerio deberán contar con autorización expresa según sea el caso y de acuerdo con los procedimientos establecidos para tal fin.
- Las áreas seguras se deberían proteger mediante controles de entrada, apropiados para asegurar que solamente se permite el acceso a personal autorizado
- Se debe autorizar el acceso al centro de cómputo, centros de cableado y centro de servidores ya que es restringido este acceso y solo debería ingresar el personal autorizado. Adicionalmente, se debe realizar el monitoreo correspondiente a estos accesos.

C. Seguridad de oficinas, recintos e instalaciones.

- Borrar la información escrita en los tableros o pizarras al finalizar las reuniones de trabajo. Igualmente, no se deben dejar documentos o notas escritas en los espacios al finalizar las reuniones.
- Garantizar que los visitantes se encuentren acompañados de un colaborador de la Municipalidad de Montes de Oro, cuando se encuentren en las oficinas o áreas seguras donde se maneje información.
- Asegurar que los visitantes que requieran permanecer en las oficinas de la Municipalidad de Montes de Oro por periodos superiores a dos días sean presentados al personal de oficina donde permanecerán.
- Portar su carné en un lugar visible mientras permanezca dentro de las instalaciones de la institución.

- En ninguna circunstancia, se debe fumar, comer o beber en las áreas seguras.
- Verificar que no se toman fotografías o grabación de video, en áreas de procesamiento de información o donde se encuentren activos de información que comprometan la seguridad o la imagen de la Municipalidad de Montes de Oro, a menos que esté autorizado.
- Verificar que las instalaciones estén configuradas para evitar que las actividades o información confidenciales sean visibles y audibles desde el exterior.

5.1.11 Dispositivos Móviles.

A. Descripción General

Evitar que los dispositivos móviles sean causa de infección y/o distribución de código malicioso.

Además de prevenir que éstos sean el origen de accesos no autorizados a las redes o recursos privados de la Municipalidad de Montes de Oro.

B. Propósito

Se debe adoptar una política y unas medidas de seguridad de soporte para gestionar los riesgos introducidos por el uso de dispositivos móviles

C. Alcance

Se aplica a todos los usuarios en la Municipalidad de Montes de Oro, incluyendo las empresas que presten servicios a la entidad.

D. Aplicación

- Llevar un registro y control de todos los dispositivos móviles (portátiles, tabletas y teléfonos móviles) que posee la Municipalidad de Montes de Oro. (Entrega y recibido de los dispositivos) y hacer firmar por parte del servidores públicos y contratistas el compromiso de cumplimiento de controles.
- Definir un procedimiento formal de salida de dispositivos de las instalaciones, donde se especifique, entre otras cosas, que el uso de los equipos portátiles de propiedad de la Municipalidad de Montes de Oro, fuera de las instalaciones, únicamente se permitirá a usuarios autorizados mediante una orden de salida, la cual debe tener el visto bueno del jefe inmediato con firma autorizada para este fin.
- Autorizar la salida de equipos de dispositivos móviles para la ejecución de actividades fuera de las instalaciones de la Municipalidad de Montes de Oro.
- No permitir la salida de equipos de escritorio para la ejecución de cualquier actividad fuera de las instalaciones de la Municipalidad de Montes de Oro. Cuando por alguna excepción se requiera la salida de un equipo de escritorio deberá tener la autorización previa del Departamento de Tecnologías de Información, con el fin de verificar que tipo de información se encuentra almacenada en el equipo.
- Contar con un sistema de autenticación, como un patrón, código de desbloqueo o una clave, para todos los dispositivos móviles, como celulares, que almacenen información de la institución.

- Mantener apagado el bluetooth o cualquier otra tecnología inalámbrica que exista o llegara a existir.
- No instalar ni configurar en los servicios ni en la infraestructura tecnológica de la institución
- Derecho a revisar la utilización del dispositivo móvil ante cualquier indicio de un uso inapropiado del mismo, inspeccionarlo o disponer de el de cualquier forma, dado que el dispositivo móvil como la información almacenada es propiedad de la Municipalidad de Montes de Oro.

5.1.12 Acceso remoto

A. Descripción General

Garantizar la seguridad de la información cuando se accede remotamente a los sistemas de información de la Municipalidad de Montes de Oro.

B. Propósito

La Municipalidad Montes de Oro debe implementar políticas y medidas de seguridad para la operación de la información a través del acceso remoto.

C. Alcance

Debe ser cumplida por todos los colaboradores en la Municipalidad de Montes de Oro y también por los colaboradores de la misma institución que presten servicios desde su domicilio.

D. Aplicación

- Contar con las aprobaciones requeridas para establecer conexión remota a los dispositivos de la plataforma tecnológica de la Municipalidad de Montes de Oro.
- Establecer conexiones remotas únicamente a través de las conexiones seguras y utilizar computadores en sitios confiables (Ej. Casa) y, en ninguna circunstancia, en computadores públicos, de hoteles o cafés internet, entre otros.
- Configurar las conexiones remotas a los servicios tecnológicos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores asignadas dentro de la Municipalidad de Montes de Oro.
- El colaborador que solicite el acceso remoto es responsable del uso adecuado del mismo.

5.1.13 Uso del Antivirus

A. Descripción General

La Municipalidad de Montes de Oro está en la obligación de proteger la información que le pertenece y que se encuentra en su custodia, de instrucciones maliciosas. Así, con el fin de mantenerse alerta ante la presencia de virus, y de poder responder adecuadamente para prevenirlos o administrar sus consecuencias, es que se aprueban estas políticas de uso de antivirus.

B. Propósito

Establecer los requerimientos que en materia de antivirus deben ser satisfechos, para todos los equipos computacionales conectados de manera lógica o física, a los sistemas informáticos o redes de la Municipalidad de Montes de Oro, a fin de prevenir y detectar de manera efectiva algún problema.

C. Alcance

Estas políticas son aplicables a todos los usuarios de equipos computacionales que hayan de ser conectados a los sistemas informáticos de la Municipalidad de Montes de Oro.

D. Aplicación

A. Uso del Antivirus y Prevención de Infestación.

1.Responsabilidad del personal con respecto a la aplicación del antivirus aprobada por la institución.

Todos los colaboradores deben tener instalada y efectivamente activa, en el equipo computacional que utiliza la Municipalidad de Montes de Oro, la aplicación antivirus formalmente aprobada, corriendo en su última versión, antes de proceder a conectarse a los sistemas de la Institución. A menos que cuente con autorización expresa y por escrito válidamente emitida para tales efectos, ningún usuario debe por su propia cuenta y por ninguna razón, deshabilitar las aplicaciones de antivirus instaladas en los equipos de la Institución. Toda instalación o desinstalación de las

aplicaciones de antivirus, será llevada a cabo únicamente por personal del Departamento de Tecnologías de Información.

2. Prohibición del personal de tratar de eliminar una instrucción maliciosa por sus propios medios.

Los colaboradores, no deben bajo ninguna circunstancia tratar de eliminar instrucciones maliciosas de los equipos o sistemas conectados a la red de la Municipalidad de Montes de Oro, por sus propios medios. Ante la mera sospecha de la existencia de una instrucción maliciosa, el usuario debe proceder inmediatamente a hacer uso de los canales formalmente aprobados para hacer el respectivo reporte, ante el Departamento de Tecnologías de Información.

3. Instalación y actualización de software antivirus en equipo aprobado.

Solamente el Departamento de Tecnologías de Información, procederá a instalar el software antivirus que la Institución haya previamente aprobado y que cuente con su respectiva licencia. Este software se instalará únicamente en aquellos equipos computacionales que haya sido, a su vez, previamente autorizados.

4. Prohibición de utilizar cualquier software no licenciado no autorizado por la Municipalidad de Montes de Oro.

A menos que expresamente se estipule lo contrario, está absolutamente prohibida la instalación y utilización de cualquier tipo de software no licenciado o no autorizado, en los equipos o sistemas conectados a la red de la Institución.

5. Archivos y software proveniente de fuentes desconocidas.

No deben ejecutarse archivos ni software que provengan de fuentes desconocidas en los equipos o sistemas conectados a la red de la Municipalidad de Montes de Oro. Siempre que se tenga motivo suficiente y fundamentado para creer que un archivo o software de fuente desconocida pueda contener información de importancia para la Municipalidad de Montes de Oro, debe contactarse inmediatamente al Departamento de Tecnologías de Información, para que este pueda accederla en un ambiente controlado.

B. Escogencia y administración de la plataforma Antivirus.

1. Escogencia y aprobación de al menos una aplicación antivirus Para la Municipalidad de Montes de Oro.

Para el desarrollo, adquisición, modificación, y actualización de sus sistemas, se debe escoger y estandarizar el uso de al menos una aplicación de antivirus que provea la protección contra instrucciones malignas que la Institución necesita. Esta aplicación debe mantenerse permanentemente actualizada y licenciada corporativamente, para todas las redes, sistemas y estaciones de trabajo, tomando en cuenta las expectativas de crecimiento de la Institución. Asimismo,

debe proporcionarse capacitación suficiente y constante a quienes administren la plataforma escogida.

2. Administración de la plataforma de antivirus.

Corresponderá al Departamento de Tecnologías de Información la administración de la plataforma de antivirus, de modo que la misma se mantenga funcionando óptimamente y permanentemente actualizada. El personal del Departamento de Informática tendrá la responsabilidad de mantenerse capacitado en la herramienta, de manera que pueda sacarle el mejor provecho en beneficio de la institución.

3. Revisión periódica de los equipos y sistemas conectados a la red de la Municipalidad de Montes de Oro a efectos de controlar instrucciones maliciosas.

En la sana administración de los sistemas y a fin de evitar y controlar instrucciones maliciosas, el Departamento de Informática debe llevar a cabo revisiones periódicas en sus sistemas y equipos, dirigidas a garantizar que los mismos se encuentran libres de códigos malignos, así como asegurar que los usuarios posean instalado el software de antivirus aprobado por la Institución.

4. Recuperación frente a virus.

Se deben contemplar entre otras cosas, provisiones para la recuperación rápida y eficiente ante ataques por virus, incluyendo protección de la información de la Institución.

5. Controles contra puertas ocultas y códigos troyanos.

Se deben establecer controles dirigidos a procurar evitar la instalación de puertas ocultas y código troyano en los sistemas de la Municipalidad de Montes de Oro.

Así, los controles mínimos que deben aplicarse serán:

- Adquirir programas únicamente de proveedores acreditados.
- Adquirir programas en código fuente de manera que el mismo pueda ser verificado.
- Utilizar productos previamente evaluados.
- Examinar todo el código fuente antes de pasar un programa a producción.
- Controlar el acceso y las modificaciones al código una vez instalado el mismo.
- Emplear personal de probada confiabilidad para trabajar en los sistemas críticos.

5.1.14 Mantenimientos de Activos.

A. Descripción General

Lo definido en la presente política aplica para el mantenimiento de los activos y asegurar una mejor protección para la información de la Municipalidad de Montes de Oro.

B. Propósito

Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.

C. Alcance

Aplica para todos los colaboradores de la Municipalidad de Montes de Oro del Departamento de Tecnologías de Información.

D. Aplicación

- Asegurar que se les efectúe mantenimiento a los equipos adecuadamente con el objeto de garantizar su disponibilidad e integridad continua.
- Asegurar el correcto funcionamiento de los equipos de cómputo, concretando tiempos de mantenimiento de los equipos con el Departamento de Tecnologías de Información y con los colaboradores.
- Sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
- Se deben mantener registros de todas las fallas supuestas o reales y de todo el mantenimiento preventivo y correctivo.
- Contemplar un mantenimiento preventivo a los servidores del centro de cómputo trimestralmente.

5.1.15 Gestión de Actualizaciones

A. Descripción General

Todo software es susceptible de necesitar actualizaciones por motivos de seguridad, esto incluye los equipos electrónicos, los sistemas operativos y aplicaciones informáticas e incluso los propios programas antivirus. Los fabricantes de software lanzan actualizaciones y parches que mejoran y añaden nuevas funcionalidades, o que corrigen errores y agujeros de seguridad.

B. Propósito

Revisar la existencia de actualizaciones y parches de seguridad para nuestro software y elaborar procedimientos que permitan que tales actualizaciones y parches sean instalados en nuestros equipos de forma segura y controlada.

C. Alcance

Se aplica a todos los colaboradores con equipos computacionales de la Municipalidad de Montes de Oro y al Departamento de Tecnologías de Información.

D. Aplicación

1. Determinar el software qué debe ser actualizado.

Tendremos que realizar un inventario de todo el software instalado, ya que pueden descubrirse errores o mejoras de funcionalidad. Para corregir dichos errores y garantizar un comportamiento óptimo debemos instalar, en cuando tengamos conocimiento de ellos, las correspondientes actualizaciones y parches de seguridad.

2. Determinar cuándo y qué actualizaciones instalar.

El departamento de Tecnologías de Información determinará el momento en que ejecutar las actualizaciones para no interferir con las operaciones de la empresa. Aunque los principales programas comerciales disponen de funcionalidades de actualización automática, cabe la posibilidad de que tengamos software instalado que no disponga de estas opciones de actualización.

Antes de su instalación el Departamento de Tecnologías considerará la utilidad de las nuevas mejoras, así como los requisitos necesarios.

3. Probar las actualizaciones.

Siempre debemos instalar actualizaciones provenientes de fuentes confiables. No obstante, se debe sopesar la necesidad de disponer de un entorno de pruebas o preproducción donde instalar y probar las actualizaciones, de este modo podremos verificar que su funcionamiento es el esperado.

4. Deshacer los cambios.

Antes de aceptar la instalación de una actualización, se debe considerar la forma de deshacer los cambios realizados. Así si el comportamiento del software actualizado no responde a lo esperado podremos volver a la situación anterior. Siempre es recomendable disponer antes de cualquier cambio de copias de seguridad recientes localizadas y probadas.

5. Herramientas de diagnóstico y actualización.

Existen herramientas que revisan si el software de nuestros equipos está actualizado o no. Una vez detectadas las actualizaciones pendientes, podemos proceder a su instalación en todos los equipos de manera centralizada. Esto puede ser útil en entornos con muchos equipos en los que queremos que el software instalado sea homogéneo y esté especialmente controlado.

6. Registro de actualizaciones.

Realizaremos un registro de las actualizaciones que se han instalado en nuestros sistemas. De esta forma podremos tener en todo momento un conocimiento exhaustivo del software operativo en nuestros equipos.

CAPITULO VI

CONCLUSIONES Y RECOMENDACIONES

El Plan Estratégico de Tecnologías de Información y Comunicaciones define las estrategias que busca la Municipalidad de Montes de Oro en el ámbito tecnológico, para implementar las normativas del MICITT, además de cerrar las brechas importantes y no solo estará enfocado en el departamento de TI, sino que tomará en cuenta a toda la empresa, con la finalidad de brindar un mejor servicio a los clientes, proveedores y personal de la institución.

La confección y preparación se originó de la necesidad que tiene la Municipalidad de Montes de Oro de cumplir con las normativas del MICITT esto con el fin de poder potenciar los recursos que tienen actualmente y poder alcanzar los objetivos de una forma más expedita.

Es importante mencionar y destacar que es fundamental, para la ejecución de manera exitosa de las estrategias tecnológicas, contar con el compromiso de todos los colaboradores de la institución.

6.1 Conclusiones

Al desarrollar este proyecto de investigación se pudo obtener con éxito la meta propuesta en relación con los objetivos propuestos al iniciar esta investigación, quedando en evidencia un análisis de la situación actual del área de tecnologías de información y comunicaciones de la Municipalidad de Montes de Oro, así como también el desarrollo de un plan de tecnologías de información y comunicaciones, siendo este último una guía que pretende generar valor a la empresa, permitiendo que se establezca una relación entre la planificación empresarial y los proyectos que se van a desarrollar por el área de tecnologías de información.

- Se obtiene que la Municipalidad de Montes de Oro no posee ningún Sistema de Gestión de Seguridad de la Información, lo que trae como consecuencia que los proyectos propuestos no están alineados a los objetivos estratégicos por

ende algunos de ellos pueden verse impactados de manera negativa, causando que se posterguen, o que no sigan en su ciclo, adicionalmente al no estar alineados a la estrategia empresarial se ve a TI como un área aparte de la empresa y no como un contribuyente lo que puede ocasionar desactualización en servicios como hardware o software.

- Se demostró que la Municipalidad de Montes de oro cuenta con un nivel tecnológico regular ya que tiene áreas de mejora y oportunidad para buscar estar en la vanguardia tecnológica para así ofrecer una mejor experiencia tanto a sus colaboradores como a sus proveedores y clientes

- Al determinar las necesidades primarias se concluye y se reafirma la necesidad de implementar un Sistema de Gestión de Seguridad de la Información, el cual tendrá como fin alinear toda la institución con las normativas sugeridas por el MICITT, a su vez mejorar las experiencias laborales de cada colaborador y también reduciendo los problemas a nivel tecnológico y empresarial.

- El tema de tiempo fue una limitante para el desarrollo del proyecto debido a que la solicitud por parte de la Municipalidad de Montes de oro incluía el desarrollo completo del Sistema de Gestión de Seguridad de la Información el cual de acuerdo a la ISO 27001 menciona que el tiempo mínimo para realizar un plan de este tipo es de entre 8 a 20 meses.

6.2 Recomendaciones

Para abordar las normativas requeridas por el MICITT, se recomienda a la Municipalidad de Montes de Oro que implemente la propuesta del Sistema de Gestión de Seguridad de la Información desarrollada en este proyecto final de graduación, buscando solventar las necesidades existentes, provocando un impacto positivo en el Departamento de Tecnologías de Información y un mejor desarrollo de las tareas de cada colaborador.

A continuación, se detallarán las recomendaciones para la institución:

- Tomar en cuenta los documentos propuestos en esta tesis, esto con el fin de poder seguir manteniendo una organización correcta y adecuada de la institución.

- Utilizar los lineamientos y las políticas que fueron propuestas como parte de este proyecto y en caso de ser necesario trabajar en ampliar dichas políticas o lineamientos.

- Una vez se tenga el visto bueno para la implementación del Sistema de Gestión de Seguridad de la Información procurar efectuar el proceso de comunicación correcta y oportuna a todos los colaboradores de la institución, siguiendo las políticas de comunicación de la misma.

- Aprovechar los diferentes diagnósticos efectuados en este proyecto en caso de querer incorporar algún otro plan de acción o proyecto, así como también se recomienda utilizar esta metodología para propuestas futuras.

- Velar que los lineamientos y las políticas se cumplan, efectuando una revisión formal del mismo de manera anual, en conjunto con los operativos anuales, de esta manera se podrá identificar los ajustes necesarios y a su vez poder ajustar el presupuesto en caso de ser necesario y aprovechar para ver el avance de los proyectos planteados.

- Finalmente se recomienda que el resto de los departamentos de la Municipalidad de Montes de Oro se unan en brindar el apoyo necesario al departamento de TI y se comprometan con el Sistema de Gestión de Seguridad de la Información para convertirse en un participante activos del mismo garantizando que la empresa marche con un mismo rumbo.

BIBLIOGRAFIA

Naranjo García, A. (2010). *Sistema de Autenticación y Control de Acceso para aplicaciones del Departamento de Soluciones para la Aduana*.[Trabajo de Diploma, Universidad de las Ciencias Informáticas]. https://repositorio.uci.cu/jspui/bitstream/ident/TD_03315_10/1/TD_03315_10.pdf

Quiroz, S. y Macías, D. (2017). Seguridad en informática: consideraciones. Dominio de las Ciencias, 3(5),677 - 688. https://dialnet.unirioja.es/descarga/articulo/6137824.pdf

Solarte Solarte, F. N., Enriquez Rosero, E. R., & Benavides, M. del C. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica, 28(5),493 - 507. http://200.10.147.88/index.php/tecnologica/article/view/456/321

Molina, Y. y Orozco, L. (2020). *Vulnerabilidades de los Sistemas de Información: una revisión.* https://dspace.tdea.edu.co/bitstream/handle/tdea/1398/Informe%20Vulnerabilidad%20sistemas.pdf?sequence=1&isAllowed=y

Silva, F, Segadas, L y Kowask, E. (2014). *Planeación y Gestión Estratégica de las TI.* [Universidad Nacional de Colombia]. https://www.cedia.edu.ec/assets/docs/publicaciones/libros/GTI8.pdf

Calderon, L. (s.f). *Seguridad informática y seguridad de la información.* [Archivo PDF]. http://polux.unipiloto.edu.co:8080/00002658.pdf

Avenía Delgado, C. (2017). *Fundamentos de seguridad informática.* Fundación Universitaria del Área Andina. https://core.ac.uk/download/pdf/326424171.pdf

Vision Solutions. (2004). *Los Fundamentos de disponibilidad Gestionada*. https://www.swgreenhouse.com/files/documents/continuidad-de-negocio/white-paper-los-fundamentos-de-la-disponibilidad-gestionada.pdf

Comisión sobre la Seguridad Humana. (2003). *Human Security Now Final Report*. Nueva York: CSH. https://www.iidh.ed.cr/multic/UserFiles/Biblioteca/IIDHSeguridad/12_2010/97c70a6a-82ff-409c-a1de-438406607896.pdf

Fernández, F., (2002). El análisis de contenido como ayuda metodológica para la investigación. Revista de Ciencias Sociales, 2(96), 35 – 53. https://www.redalyc.org/pdf/153/15309604.pdf

Rea Guamán, A. (2020). *Madurez en la Identificación y Evaluación de Riesgos en Ciberseguridad*.[Tesis Doctoral, Universidad Politécnica de Madrid]. https://oa.upm.es/65871/1/ANGEL_MARCELO_REA_GUAMAN.pdf

Organización Internacional de Normalización. (2013). *Aspectos clave de su diseño e implantación* (ISO 27001).

ESAN Graduate School of Business. (05 de mayo de 2016). ¿Qué es el Business Continuity Management (BCM)?. https://www.esan.edu.pe/conexion-esan/que-es-el-business-continuity-management-bcm#:~:text=El%20Business%20Continuity%20Management%20(BCM)%20se%20puede%20definir%20tambi%C3%A9n%20como,limita%20al%20campo%20del%20diagn%C3%B3stico.

La Asociación Española para el Fomento de la Seguridad de la Información.(08 de Enero 2021). ¿Qué son los Personal Information Management Systems (PIMS)?. https://www.ismsforum.es/noticias/1712/qu-son-los-personal-information-management-systems-pims-n/

Deloitte. (2016). *Ciberseguridad para personal no técnico* (Deloitte Touche Tohmatsu Limited).

Malwarebytes. (2022). *Todo acerca del malware*. https://es.malwarebytes.com/malware/

Ocampo, C. (2007) Sistema de detección de intrusos en redes corporativas. Scientia Et Technica, *22, P.61*. Recuperado de https://www.redalyc.org/pdf/849/84953102008.pdf

ESET. (2022). *¿Qué es un antivirus?* https://www.eset.com/es/caracteristicas/antivirus-software-que-es/

Stocking, Geoge W. 1993 La Magia del Etnógrafo. El Trabajo de Campo en la Antropología Británica desde Tylor a Malinowski, en Lecturas de Antropología para Educadores. Editorial Trotta, Madrid

Barrantes, R. (2014). *Investigación, Un camino al conocimiento, Un Enfoque Cualitativo, Cuantitativo y Mixto.* San José, Costa Rica, Editorial EUNED.

Cook, T. D. y Reichardt, CH. S. 1979. Qualitative and quantitative methods in evaluation research. Beverly Hills, California, USA.

Voutssas M., J. (2010). Preservación documental digital y seguridad informática. Investigación Bibliotecológica, 24(50), 127-155. Recuperado de: http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008&lng=es&nrm=iso.

Hernández, R.; Fernández, C. & Baptista, P. (2006). Metodología de la Investigación. México: Mc Graw-Hill Interamericana S.A.

Arias, F. (2006). El Proyecto de Investigación: Introducción a la Metodológica Científica. Caracas: Espíteme.

Marroquín, P. R. (2012). Matriz operacional de la variable y matriz de consistencia. Recuperado de http://www.une.edu.pe/diapositivas3-matrizde-consistencia-19-08-12.pdf

MUNICIPALIDAD DE MIRAMAR

MUNICIPALIDAD DE MIRAMAR: SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN

SGSI

Municipalidad de Miramar

Cantón de Montes de Oro

1.Sistema de Gestión de Seguridad de la Información.

Este documento describe cómo debe ser realizada la gestión de la seguridad de información por la Municipalidad de Montes de Oro para un mejor funcionamiento de la institución y respetando las directrices que le solicita el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones.

2.Elaboración de Políticas.

Las políticas del Sistema de Gestión de Seguridad de la Información consisten en definir acuerdos de nivel de servicio entre los colaboradores y responsables del Departamento de Tecnologías de Información, de tal forma que se desarrolle el proceso con total normalidad rigiéndose a los acuerdos realizados. A continuación, se definen las implicaciones de la política:

- Los miembros del Departamento de TI de la empresa deberán comprometerse a colaborar y a participar activamente en la elaboración de las políticas brindando toda la información necesaria de la misma.
- Los miembros del Departamentos de Tecnologías de Información se comprometen a manejar con estricta confidencialidad la información que les sea proporcionada y referente a la empresa.
- El Departamento de Tecnologías de Información determinará personas claves de la empresa quienes serán los que proporcionen la mayor cantidad de la información que se requiere para elaborar la política.
- Cada política se detallará de la siguiente manera: Descripción General, Propósito, Alcance y Aplicación.

3. Políticas de Seguridad.

En este apartado se describen las políticas de seguridad que se utilizaran para un mejor funcionamiento de la institución y respetando las directrices que le solicita el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones.

3.1 Roles y responsabilidades

A. Descripción General

La identificación de los roles y responsabilidades en la Municipalidad de Montes de Oro, permite establecer al interior de la entidad las acciones correspondientes para proteger los activos de información, reduciendo posibles eventos y/o incidentes de seguridad de la información. De esta manera los colaboradores de la entidad, adquieren el compromiso de protegerlos y se hacen partícipe de las actividades e iniciativas encaminadas al aseguramiento de los recursos que se encuentran bajo su custodia.

B. Propósito

Definir roles y responsabilidades para la atención de incidentes adversos que afecten la seguridad de la información de la Municipalidad de Montes de Oro.

C. Alcance

El presente documento describe los roles y responsabilidades de los encargados de la Seguridad de la información de los diferentes procesos de la Municipalidad

de Montes de Oro, conservando la confidencialidad, integridad y disponibilidad de la Información. Por lo anterior, todos los colaboradores de la Municipalidad de Montes de Oro serán responsables de la identificación, evaluación y control de los riesgos de seguridad de la información.

D. Aplicación

Para lograr el buen funcionamiento de la seguridad y privacidad de la Información, la entidad particularizará los roles y responsabilidades de los colaboradores de la entidad que se van a encargar de establecer y desarrollar cada una de estas actividades asociadas a los sistemas.

Para la asignación de los responsables, la Municipalidad de Montes de Oro, analizará las funciones de cada rol relacionándolas con las actividades que realiza el personal de la entidad, por lo anterior, para cada perfil, serán incorporadas los manuales de funciones en las obligaciones de los contratos por prestación de servicios de acuerdo con el cargo que desempeñan.

A continuación, se definen algunos roles y responsabilidades que se deben tener en cuenta en la implantación y seguimiento del Sistema de Gestión de Seguridad de la Información.

Comité Institucional de Gestión y Desempeño.

Como muestra de su compromiso en la dirección, gestión y apoyo en la seguridad y privacidad de la Información, aprueba lo siguiente:

Aprobar anualmente o cuando se requiera la Política de Seguridad y Privacidad de la Información de la entidad.

Asignar y aprobar el presupuesto necesario para la implantación y posteriormente el normal funcionamiento y/o puesta en marcha del Sistema de Gestión de Seguridad de la Información.

Garantizar que los requisitos del Sistema de Gestión de Seguridad de la Información se encuentran integrados en todos los procesos críticos de la entidad.

Proporcionar los recursos necesarios para la implementación y desarrollo de las actividades del Sistema de Gestión de Seguridad de la Información en la entidad.

Velar por la ejecución y desarrollo de las actividades del Sistema de Gestión de Seguridad de la Información.

Promover activamente una cultura de seguridad y privacidad de la información basada en riesgos para la entidad.

Aprobar los roles y responsabilidades relacionados con la seguridad de la información en todos los niveles de la entidad.

Especialista Seguridad de la Información

Es el responsable de la Seguridad de la Información en la entidad, el cual debe pertenecer a un área que haga parte de la Alta Dirección. Así mismo, debe pertenecer e informar al Comité Institucional de Gestión y Desempeño todo lo referente al Sistema de Gestión de Seguridad de la Información, al cual asistirá en forma oportuna y garantizará el mejoramiento continuo de cualquier necesidad de mejora respecto a la seguridad y privacidad de la información de la entidad.

Emitir conceptos referentes a riesgos y seguridad de la información de la entidad, para la toma de decisiones por parte del Comité Institucional de Gestión y Desempeño.

Coordinar la implementación, despliegue y sostenibilidad del Sistema de Gestión de Seguridad de la Información.

Mantener una comunicación clara, oportuna, completa y permanente con los diferentes roles.

Definir las herramientas, metodologías y lineamientos necesarios para la implementación de la seguridad y privacidad de la Información.

Verificar que se incluyan los temas asociados a la seguridad y privacidad de la Información, dentro del plan de capacitaciones de la entidad.

Asegurar que se definan e implementen actividades de sensibilización y concienciación frente a la seguridad de la información a la Alta Dirección y demás partes interesadas.

Guiar a la Alta dirección de la entidad, ante incidentes de seguridad mediante el plan de respuesta de incidentes.

Responsable de la elaboración y desarrollo del Plan de Seguridad de la Información.

Mantener contacto con grupos de interés.

Mantener y promover la actualización de las políticas de seguridad de la información.

Debe responder por la revisión de problemas de seguridad de la información existentes y aquellos que se consideren potenciales.

Responsabilidades Colaboradores

Es responsabilidad de todos los colaboradores, que tengan acceso a la información de la Municipalidad de Montes de Oro, cumplir con todas las políticas y procedimientos definidos frente a la protección de la información, las cuales le han sido suministrados para la labor designada y así mismo usar de manera segura los documentos de información que le fueran asignados. Estos

colaboradores deben estar autorizados por el responsable, quien será el gestor del control y vigilancia del uso adecuado de los activos de información. Los colaboradores deben aceptar por escrito los términos y condiciones de uso de la información, así como el cumplimiento estricto de las políticas de seguridad de la información de la entidad antes de su acceso a los mismos.

3.2 Cifrado e Información Confidencial

A. Descripción General

Dado a la naturaleza de la información que se maneja en la Municipalidad de Montes de Oro, se debe considerar la sensibilidad de los datos que residen en los sistemas de información para el debido control y acceso. Pérdida o mal uso de esta información puede resultar en una variedad de daños, tales como pérdida de confidencialidad e incumplimiento de regulaciones y leyes aplicables a la entidad.

B. Propósito

Establecer normas para el uso de algoritmos de encriptación y servicios de protección de información a utilizar en la Municipalidad de Montes de Oro y para el uso, protección y vida útil de las claves criptográficas durante toda su vida útil en cumplimiento con todos los acuerdos, la legislación y las normativas pertinentes.

C. Alcance

Esta política se aplica al uso de algoritmos de cifrado como herramientas de control, protección de la confidencialidad, autenticidad o integridad de la información, así como la debida documentación y resguardo de estos.

Debe ser cumplida por todos los usuarios en la Municipalidad de Montes de Oro, incluyendo las empresas que presten servicios a la entidad.

D. Aplicación

Generalidades

Se debe cifrar toda la información sensible, clasificada como confidencial, que pudiese quedar expuesta a usuarios no autorizados, en relación con su privacidad e integridad.

Se deben utilizar controles criptográficos para la protección de la confidencialidad, el cumplimiento del principio de la no repudiación y el control de integridad de la información en los siguientes casos:

Protección de claves de acceso a sistemas, documento electrónico, datos y servicios.

Transmisión de información clasificada fuera del ámbito del servicio.

Resguardo de información cuando así surja de la evaluación de riesgos realizada por el propietario de la información y el encargado de seguridad de la información.

Acerca de la confidencialidad

Se definen los algoritmos de cifrado que podrán utilizarse al interior de la Municipalidad de Montes de Oro, como una aplicación directa o como parte de la configuración de otros productos de seguridad comerciales, tomando en cuenta el tipo y la calidad del algoritmo de cifrado utilizado y la longitud de las claves

criptográficas. Sólo se utilizan algoritmos de cifrado definidos en estándares internacionales.

Acerca de la integridad/autenticidad

Para verificar la autenticidad o integridad de la información almacenada o transmitida sensible o crítica, la Municipalidad de Montes de Oro utiliza como mecanismo criptográfico la firma digital bajada en certificados digitales. En el caso de documentos electrónicos, estos son de carácter de firma electrónica avanzada.

Acerca de la Autenticación

Se utilizan técnicas criptográficas para autenticar a los usuarios o entidades externas que requieren hacer uso de los sistemas de información de la Municipalidad de Montes de Oro. Los funcionarios deben usar el sistema autorizado por la Municipalidad de Montes de Oro para efecto de autenticación.

El encargado de seguridad debe ser informado inmediatamente en caso de que se reciba cualquier comunicado por cualquier medio de comunicación de parte de una autoridad de protección de datos u otro ente regulador.

Registro y cancelación de registro de usuarios

Este mecanismo de autentificación (claves de acceso, dispositivo u otro) debe ser asignado individualmente, quedando prohibido el uso de un nombre de usuario ajeno o facilitar el usuario y su contraseña personal a un tercero.

El Departamento de Gestión de Personas es responsable de notificar por escrito al Departamento de Informática y Telecomunicaciones sobre el ingreso, salida o traslado de un usuario. Esto con el fin de que se creen, inhabiliten, modifiquen o eliminen privilegios de acceso a las diferentes plataformas, documentación, dominios y dispositivos correspondientes.

Uso de la información de autenticación secreta

Todos los funcionarios que presten servicios a la Municipalidad de Montes de Oro tienen la obligación de cumplir con las siguientes directrices:

- Mantener la información de autenticación secreta como confidencial, asegurándose de que no se divulgue a ninguna otra parte, incluidas las personas con autoridad.

- Evitar mantener un registro (es decir, en papel, archivo de software o en un dispositivo de mano) de la información de autenticación secreta.

- Cambiar la información de autenticación secreta cuando exista alguna sospecha de que pudiera haber sido vulnerada o conocida por terceros.

- No se debe compartir la información de autenticación secreta de usuario de una persona.

Contraseñas en Dispositivos de Red

Todos los dispositivos de red (routers, firewalls, switches) deben tener contraseñas únicas u otro mecanismo de control de acceso.

Si un dispositivo no posee contraseña de acceso, se debe impedir su administración remota, permitiendo la intervención sólo al personal autorizado y en forma directa (conexión local).

Contraseña por Omisión y recordatorios de contraseña

Toda contraseña por omisión provista por el fabricante de cualquier sistema debe ser reemplazada inmediatamente.

Queda absolutamente prohibido anotar las contraseñas de acceso en lugares públicos.

Cualquier contraseña encontrada en estos medios debe ser informada al encargado del Departamento de informática y tratada como un incidente.

Acceso a Información Sensible

En el caso del control de acceso a información, se deben utilizar contraseñas robustas seguras o cifradas.

La contraseña nunca debe ser compartida o revelada; hacer esto responsabiliza al usuario que prestó la contraseña de acceso y a todas las acciones que se realicen de la misma.

Frente a la evidencia de un compromiso del sistema por uso indebido de cuentas con privilegios, todas las contraseñas de cuentas con privilegios del sistema deben ser reemplazadas y se debe registrar como un incidente de seguridad.

3.3 Gestión de cuentas

A. Descripción General

La Municipalidad de Montes de Oro considera indispensable regular la creación, suspensión, reactivación, eliminación de usuarios de red y correo electrónico.

B. Propósito

El objetivo de la política es regular la creación, suspensión, reactivación, eliminación de usuarios de red y de correo electrónico, para lo cual, se emiten los siguientes lineamientos que son de cumplimiento obligatorio para todo el personal de la Municipalidad de Montes de Oro.

C. Alcance

Es necesario que todos los usuarios estén enterados y conscientes de los compromisos, normas y reglamentos que se dictan para la creación de este tipo de cuentas, tomando todas las medidas que correspondan, para que estas se respeten y se cumplan, ya que las cuentas de red y correo electrónico dan acceso a gran variedad de recursos informáticos que deben manejarse con cautela

El uso de la red y recursos de información, están disponible para fortalecer el flujo de información interna, la investigación y el apoyo a las diferentes tareas encomendadas para mejoramiento de nuestras labores. Todos los usuarios de la red están sujetos a esta política y a los términos de esta. El uso inapropiado de la red podría ser sancionado con la eliminación del acceso a estos recursos y puede

conllevar a la aplicación de las sanciones disciplinarias respectivas, además de las consecuencias de índole legal que sean aplicables.

D. Aplicación

1. Solicitud de creación de usuarios de red y correo electrónico.

Para la creación de usuarios nuevos de red y de correo electrónico, se deben seguir los siguientes pasos:

1. Debe existir una solicitud expresa por parte del Departamento de Recursos Humanos para usuarios en el Departamento de Tecnologías de Información, solicitando la creación de los accesos. Esta solicitud debe incluir al menos lo siguiente:

- Nombre completo de la persona
- Número de Identificación: Cédula Nacional, Cédula de Residencia o Pasaporte.
- Indicar si es un funcionario interino, en propiedad o un pasante.
- En caso de ser un funcionario en situación interina o pasante, se debe indicar una fecha de finalización de las labores, con el fin de limitar el acceso a los recursos informáticos hasta la fecha que se indique.
- Departamento al que pertenece el nuevo funcionario.

2. Una vez recibida la solicitud en el Departamento de Tecnologías de Información, se procederá a realizar la creación del usuario de red y del correo electrónico. El usuario de red será creado a partir del número de identificación brindado en la solicitud. También, se creará una cuenta de correo electrónico que consta de:

- Una dirección electrónica con la forma usuario@municipalidadmontesoro.go.cr.

- Una palabra clave o contraseña para acceder de manera privada a la cuenta.
- La posibilidad de enviar y recibir mensajes en la Intranet y hacia Internet utilizando la dirección electrónica asignada.

3. Dadas las limitaciones de cuentas con que cuenta el Departamento de Tecnologías de Información, sólo se crearán cuentas de correo para funcionarios interinos o en propiedad, limitando el acceso a estas a las personas que realicen pasantías en la Institución.

4. Todo usuario para tener acceso a los recursos de red y al correo electrónico, deberá quedar registrado en la Base de Datos de Usuarios de red del Departamento de Tecnologías de Información.

5. Una vez creados los accesos correspondientes, el Departamento de Tecnologías de Información se encargará de notificar la cuenta y clave de acceso, al responsable de la solicitud para que la retire en las oficinas del Departamento de Recursos Humanos. Las claves creadas por el Departamento son temporales, por lo que se deben cambiar en el primer ingreso del usuario. La nueva clave debe cumplir con las siguientes características:

- Tamaño mínimo de 8 (ocho) caracteres.
- Utilizar letras mayúsculas (de la “A” a la “Z”), minúsculas (de la “a” a la “z”), números (del “0” al “9”) y preferiblemente caracteres especiales como $, #, &, * (asterisco) y (punto).
- No se permitirá claves en blanco.
- Evitar el uso de su nombre, sus apellidos, nombres de personas, animales, iniciales familiares, cédulas.
- No usar secuencias básicas de caracteres que cambian parcialmente con base en la fecha u otro factor fácilmente predecible.
- Se recomienda realizar un cambio de contraseña por lo menos una vez cada 30 días naturales.

- Es importante aclarar que la misma contraseña del usuario de red es la que se utiliza para acceder al correo electrónico

2. Solicitud de suspensión temporal de usuarios de red y correo electrónico.

Para la suspensión temporal de usuarios de red y de correo electrónico, se deben seguir los siguientes pasos:

1. Se puede dar por motivos de seguridad informática ante el conocimiento previo del Departamento de Tecnologías de Información respecto a la separación del cargo, de algún funcionario de la institución, ya sea este por motivos de despido, suspensión temporal, permiso sin goce se salario, u alguna otra situación contemplada por la gestión de Recursos Humanos. También puede darse una suspensión temporal de los accesos si se detecta desde el Departamento de Tecnologías de Información, algún acceso indebido u otro evento que pueda afectar la integridad y seguridad de las cuentas del funcionario. O bien, mediante la tramitación inmediata de una solicitud expresa por parte del Departamento de Recursos Humanos, por medio de un correo electrónico para el Departamento de Tecnologías de Información, solicitando la suspensión de los accesos. Esta solicitud debe incluir al menos lo siguiente:

- Nombre completo de la persona
- Número de Identificación: Cédula Nacional, Cédula de Residencia o Pasaporte
- Indicar si es un funcionario interino o en propiedad.
- Departamento al que pertenece el nuevo funcionario.
- Fecha a partir de la cual se hace una suspensión temporal de los accesos.

2. Seguidamente se procederá a realizar la suspensión del usuario de red y del correo electrónico, manteniéndose en dicho estado hasta que no exista una solicitud de reactivación o eliminación de la cuenta en definitiva por parte de Recursos Humanos.

3. Solicitud de reactivación de una cuenta de usuarios de red y correo electrónico suspendida.

Para la reactivación de usuarios de red y de correo electrónico, se deben seguir los siguientes pasos:

1. Debe existir una solicitud expresa por parte del Departamento de Recursos Humanos, por medio de un correo electrónico para el Departamento de Tecnologías de Información, solicitando la reactivación de los accesos. Esta solicitud debe incluir al menos lo siguiente:

- Nombre completo de la persona.
- Número de Identificación: Cédula Nacional, Cédula de Residencia o Pasaporte.
- Indicar si es un funcionario interino o en propiedad.
- Departamento al que pertenece el nuevo funcionario.
- Fecha a partir de la cual se debe hacer la reactivación de los accesos.

2. Una vez recibida la solicitud en el Departamento de Tecnologías de Información, se procederá a realizar la reactivación del usuario de red y del correo electrónico, a partir de la fecha que se indique en la solicitud.

4. Solicitud de eliminación de una cuenta de usuarios de red y correo electrónico suspendida.

Para la eliminación de usuarios de red y de correo electrónico, se deben seguir los siguientes pasos:

1. Debe existir una solicitud expresa por parte del Departamento de Recursos Humanos, por medio de un correo electrónico para el Departamento de Tecnologías de Información, solicitando la eliminación de los accesos. Esta solicitud debe incluir al menos lo siguiente:

- Nombre completo de la persona.
- Número de Identificación: Cédula Nacional, Cédula de Residencia o Pasaporte.
- Indicar si es un funcionario interino o en propiedad.
- Departamento al que pertenece el nuevo funcionario.
- Fecha a partir de la cual se debe hacer la reactivación de los accesos.

2. Una vez eliminados los accesos, el usuario tendrá 30 días naturales (1 mes calendario), para que pueda solicitar un respaldo de su correo electrónico, esto antes de que su cuenta sea eliminada por completo del sistema de correo electrónico institucional.

5. Responsabilidades.

1. Cada usuario y funcionario es responsable de los mecanismos de control de acceso a la red, que les sean proporcionados; esto es, de su “Usuario” (número de cédula del funcionario) y contraseña necesarios para acceder a la red interna de información y a la infraestructura tecnológica de la Municipalidad de Montes de Oro, por lo que se deberá mantener de forma confidencial.

2. Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por el Departamento de Tecnologías de Información antes de poder usar la infraestructura tecnológica de la Municipalidad de Montes de Oro.

3. Los usuarios no deben proporcionar información a personas externas, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica de la Municipalidad de Montes de Oro.

4. Cada usuario que acceda a la infraestructura tecnológica de la Municipalidad de Montes de Oro, debe contar con un identificador de usuario (número de cédula) único y personalizado. Por lo cual, no está permitido el uso de un mismo identificador por varios usuarios.

5. Los usuarios y funcionarios son responsables de todas las actividades realizadas con su identificador de usuario (ID). Los usuarios no deben divulgar ni permitir que otros utilicen sus identificadores de usuario, ni tampoco utilizar el ID de otros usuarios.

6. La asignación de contraseñas debe ser realizada de forma individual, y por tanto no debe ser compartida. Hacer esto responsabiliza al usuario que prestó su contraseña de todas las acciones que se realicen con su cuenta de correo.

7. Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá apersonarse al Departamento de Tecnologías de Información para que se le proporcione una nueva contraseña.

8. Las contraseñas no deben registrarse o anotarse en un lugar donde personas no autorizadas puedan descubrirlos, tampoco se deben almacenar en ningún programa o sistema que proporcione esta facilidad y que pueda ser utilizado por terceras personas.

9. Por seguridad de la información nunca se debe utilizar opciones de los sistemas para “recordar las contraseñas”, esto por cuanto el acceso queda directo y cualquier persona que ingrese a ese equipo podría hacer uso de esa cuenta de correo

10. Todo usuario que tenga la sospecha de que su contraseña es conocida por otra persona, deberá cambiarlo inmediatamente.

11. No utilice comandos o programas o el envío de mensajes de cualquier tipo con el propósito de interferir o deshabilitar una sesión de usuario a través de cualquier medio, local o remoto (Internet o Intranet).

6. Uso y administración del correo electrónico.

A. La cuenta de correo electrónico

Se entiende por cuenta de correo electrónico la asignación por parte de la Municipalidad de Montes de Oro:

- Una dirección electrónica con la forma usuario@municipalidadmontesoro.go.cr.
- Un buzón (espacio en disco) para almacenar los mensajes.
- Una palabra clave o contraseña para acceder de manera privada a la cuenta.
- La posibilidad de enviar y recibir mensajes a buzones de otras plataformas de correo, dentro y fuera del país.
- Formato de las cuentas de Usuario: Con el fin de garantizar que la identificación del usuario en la dirección de correo sea única, se seguirán las siguientes reglas para construir cada identificación: se formará con la primera letra del nombre del usuario y el primer apellido (sin tildes, mayúsculas, ni signos propios de algunos idiomas). En caso de presentarse coincidencias en la identificación de dos usuarios se resolverá de acuerdo con el orden de procesamiento: el primer usuario recibirá la identificación antes mencionada, al segundo usuario se le asignará la primera letra del nombre del usuario, el primer apellido, y la primera letra del segundo apellido.
- La primera vez que un usuario reciba su cuenta de correo, deberá cambiar su clave.
- Para reportar problemas o realizar cualquier solicitud que tenga relación con cuentas de correo o el servicio de correo electrónico en general, se debe hacer la correspondiente solicitud de servicio en la Intranet.
- Es responsabilidad de cada usuario tener copias de respaldo de los mensajes de sus carpetas de correo y de su agenda de direcciones electrónicas.

B. Buen uso del correo electrónico.

En la Municipalidad de Montes de Oro deberá utilizarse para trabajar solamente el correo oficial institucional, excluyendo servicios comerciales como Hotmail, Yahoo, Gmail, entre otros.

Es responsabilidad de los usuarios:

- Usar su cuenta con fines laborales de acuerdo con las funciones propias del puesto que le ha sido asignado en la Municipalidad de Montes de Oro.
- Se debe utilizar el logo institucional

C. Seguridad de la información.

Tome en cuenta las siguientes medidas de Seguridad:

- Antes de responder un mensaje, asegúrese que vaya dirigido a usted.
- Cerciore antes de contestar un mensaje, de que conoce la dirección.
- No envíe ni contestes cadenas de correo o cualquier otro esquema de "pirámide" de mensajes.
- No use su cuenta para fines comerciales.
- Analice y verifique cada correo antes de abrirlo, aun cuando cree conocer la cuenta que le envío el mensaje, por ningún motivo se deben abrir correos malintencionados tipo “phishing”.
- Debe borrar de inmediato cualquier mensaje que sea sospechoso, para no exponer el correo Institucional a un posible ataque o hurto de información.
- Nunca proporcione información confidencial por correo, ni facilite usuarios o contraseñas, de ningún tipo.
- Los usuarios no deben leer correo ajeno ni generar o enviar correos electrónicos a nombre de otra persona sin autorización o suplantándola.
- Nunca se inscriba a listas de correos que no conozca.
- La Municipalidad de Montes de Oro se reserva el derecho de monitorear mediante el Departamento de Tecnologías de Información las cuentas que presenten un comportamiento sospechoso.
- Con el fin de agilizar el envío de información, no se podrán enviar mensajes masivos, a menos que sea un asunto oficial.
- No se debe falsificar, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.
- No se debe interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.
- No envíe mensajes a gente que no conoce, a menos que exista una razón de peso de por medio
- No envíe mensajes ofensivos, abusivos, etc.

3.4 Manejo de Información

A. Descripción General

Describir las actividades que adquieren cada uno de los colaboradores de la Municipalidad de Montes de Oro con relación al manejo de la información.

B. Propósito

Tiene como propósito describir las actividades, procedimientos y responsabilidades de los colaboradores de Municipalidad de Montes de Oro con relación al manejo de la información personal de sus usuarios, así como todas las medidas de seguridad que se adoptan para la protección de la información y las normas que rigen las diferentes actividades aquí comprendidas.

C. Alcance

Comprende todos los procesos de la empresa que captan, manipulan y comparten información hasta su disposición final.

D. Aplicación

A. Identificación Y Autorización.

- Cada uno de los colaboradores de la Municipalidad de Montes de Oro se identifica en el Sistema de la Institución con un usuario y contraseña.

- El cargo que tenga cada empleado, definirá el nivel de permisos que tiene para ingresar, consultar y actualizar información.
- Para el Servidor de Archivos, se definen los documentos que pueden ser de acceso interno y los que requieren un permiso exclusivo que son almacenados en carpetas privadas, de lectura y de edición.

B. Control de Acceso.

- Bajo los mecanismos de identificación y autorización establecidos se evitará que un usuario pueda acceder a recursos a los cuales no tiene autorización.
- Los niveles de acceso a las bases de datos y al Servidor de Archivos se definen de acuerdo al perfil del cargo, en caso de que se cree un cargo nuevo se debe establecer primero el perfil para identificar el nivel de seguridad y acceso que se necesita para el ingreso.
- Cuando un empleado se retira de la Municipalidad de Montes de Oro, el Departamento de Recursos Humanos debe notificar al Departamento de Tecnologías de Información para que desactive el usuario en los diferentes sistemas.
- En caso de requerir acceso especial y el cargo no lo posea, el empleado lo solicita al Departamento de Tecnologías de Información quien analiza la petición y de ser procedente asignará los permisos.

C. Registro de Acceso.

Siempre que se realice una modificación a los datos contenidos en el Sistema de la Institución se registra identificando: la información modificada, hora y fecha de modificación, usuario que modificó y desde que equipo se realiza la modificación.

Los datos del registro de modificación, anulación y eliminación se conservan indefinidamente y solo el personal autorizado, tiene acceso en modo de consulta al módulo de auditoría del Sistema de la Institución.

Para el caso de la información almacenada físicamente en el Archivo central, se hace la solicitud de acceso a la documentación requerida al Departamento de Tecnologías de Información de acuerdo al protocolo de acceso que se tenga establecido.

D. Acceso a Datos a Través de Redes de Comunicaciones.

Las bases de datos de la Municipalidad de Montes de Oro, solo serán accesibles estando conectados a la red interna, además, tanto el Servidor de Archivos como el Sistema de la Institución tienen medidas de seguridad que limitan el acceso a la información y el nivel de permisos que se tenga para la modificación de la misma.

Los accesos al Sistema de la Institución serán controlados a través de usuario y clave personal que posee cada uno de los empleados de la Municipalidad de Montes de Oro, los cuales se gestionan de acuerdo al nivel de permiso que se requiera según el perfil del cargo que ocupa el colaborador y le dan acceso restringido a tipo de información necesaria para el desarrollo de sus actividades laborales.

El Servidor de Archivos cuenta con acceso restringido a la información de acuerdo a lo que disponga el colaborador encargado de la información, contando con archivos privados de cada área en particular e información que se permite compartir, alguna con objetivos de edición y otra con objetivos de solo lectura

E. Copias de Respaldo y Recuperación.

La creación y actualización de datos se lleva en los Sistemas de la Institución, los cuales se almacenan directamente en servidores, estos están configurados para realizar copias de seguridad diarias, se transfieren al finalizar el día a un disco duro externo y se clasifican en tres grupos:

- Abuelo: contiene los respaldos mensuales por año y el del último mes del año inmediatamente anterior.
- Padre: contiene los respaldos semanales (viernes de cada semana).
- Hijo: contiene el respaldo realizado día a día de lunes a viernes.

Los procedimientos establecidos para las copias de respaldo y para su recuperación garantizarán su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. El responsable de la información verificará semestralmente los procedimientos de copias de respaldo y recuperación de los datos. Las pruebas anteriores a la implantación o modificación de sistemas de información se realizarán con datos reales previa copia de seguridad, y garantizando el nivel correspondiente al tratamiento realizado.

F. Información y Obligaciones del Personal.

Para asegurar que todas las personas conocen las normas de seguridad que afectan al desarrollo de sus funciones, serán informadas de acuerdo con el siguiente procedimiento:

- En el momento de realizar la inducción y entrenamiento, el encargado de realizarla debe socializar con los diferentes colaboradores bajo su cargo las medidas que afectan en el desarrollo de las actividades de su ejercicio laboral.

- A través del medio interno de comunicación, se recordará periódicamente la existencia de las normas de seguridad y las consecuencias de su incumplimiento.
- Una vez al año, el responsable de Tecnologías de Información realiza una reunión con todo el personal para socialización y refuerzo del conocimiento de las medidas de seguridad de manejo de la información.

G. Funciones y Obligaciones del Personal.

Constituye una obligación del personal notificar al Departamento de Tecnologías de Información las incidencias de seguridad de las que tengan conocimiento respecto a los recursos protegidos.

Todas las personas deberán guardar confidencialidad sobre los datos personales que conozcan en el desarrollo de su trabajo, compromiso pactado en el contrato laboral de trabajo y/o de prestación de servicios.

Funciones y obligaciones de los colaboradores de la Municipalidad de Montes de Oro:

- Velar por el cumplimiento de las medidas de seguridad de la información al interior de la empresa, gestionar el conocimiento de dichas medidas y las consecuencias del incumplimiento de las mismas.
- Gestionar y verificar que los cargos asociados a su área posean los permisos para acceder a la información contenida en las bases de datos necesarias para el desempeño de sus actividades laborales.
- Velar por la adecuada disposición y el mantenimiento integral de la información, por parte del personal de la organización que requiera los documentos.

- Conocer y respetar las normas y procedimientos para el adecuado uso de la información tanto física como virtual de los usuarios de la Municipalidad de Montes de Oro.

El personal que realice trabajos que no impliquen el tratamiento de datos personales tendrán limitado el acceso a estos datos, a los documentos que contengan o a los recursos del Sistema de la Institución.

Cuando se trate de personal ajeno a Institución, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales.

En caso que por la naturaleza de las actividades desarrolladas por el contratista y necesite acceder a información personal, en el contrato se expresa la obligación de confidencialidad respecto a aquellos datos que hubiera podido conocer durante la prestación del servicio.

3.5 Gestión del cambio

A. Descripción General

Todo cambio sobre un activo y/o elemento de configuración en los ambientes de producción debe realizarse mediante una solicitud de cambio, es decir que debe registrarse y gestionarse con el Departamento de Tecnologías de Información.

Todo cambio debe tener un técnico responsable asignado, quien desempeña el rol de gestor del cambio.

B. Propósito

El objetivo es definir y establecer directrices que le permitan a la universidad evaluar los cambios internos y externos sobre el Sistema de la Institución, minimizando la aparición de nuevos riesgos en el entorno laboral a medida que suceden los cambios.

C. Alcance

Se debe o puede incluir cambios en todos los servicios, arquitecturas, procesos, herramientas, métricas y documentación para la gestión de cambios en Infraestructura y Operaciones de TI.

D. Aplicación

1. Identificar el tipo de cambio.

Se debe identificar, describir, clasificar y justificar el cambio de este procedimiento.

2.Analizar el impacto del cambio al sistema de gestión de seguridad.

Identificar y evaluar el impacto y los riesgos a los que se enfrenta el proceso con la implementación del cambio previsto, teniendo en cuenta los efectos o consecuencias del cambio y establecer los controles para minimizar riesgos e impactos.

3.Registrar las actividades del plan de gestión de cambios.

Luego de identificados los posibles impactos y riesgos, se realiza el plan de intervención o plan de gestión del cambio que debe incluir: actividad, responsable, comunicación, fecha seguimiento, estado del cambio (en ejecución o cerrado) si fue eficaz: (si /no)

4.Comunicar el plan de gestión de cambios a los interesados.

Comunicar el plan de gestión del cambio, para que conjuntamente trabajen con el responsable del proceso.

5.Implementar el plan de gestión de cambios.

Los responsables deben informar sobre las novedades que se generen en el proceso de implementación de acciones con el fin de tomar decisiones respecto a dichas novedades para que los riesgos derivados del cambio no se materialicen o los impactos se minimicen.

Cada vez que se realice un cambio en el Sistema de la Institución, se tendrá en cuenta la identificación de peligros, valoración de riesgos e identificación de aspectos e impactos.

Cuando se trate de cambios en la documentación, deberán ser difundidos según la matriz de comunicaciones de la Institución. Así mismo, cuando se trate de cambios en el perfil de cargo, se deberá informar a cada colaborador, con el fin de garantizar su entendimiento.

Cuando se trate de activos, se establecerá un procedimiento para la operación de la misma el cual estará orientado a un manual de operaciones o, además se establecerá los controles en la matriz de peligros; se debe asegurar que el colaborador que vaya a utilizar el activo entienda la forma de operación y los riesgos y los controles y si es posible tratar que el trabajador reciba el entrenamiento directamente del fabricante o el distribuidor del activo.

3.6 Gestión de incidentes

A. Descripción General

Contar con una política de gestión de incidentes es clave para garantizar la supervivencia de la empresa ante los efectos negativos causados por un ataque de ciberseguridad. Es fundamental diseñar un plan que determine el alcance de las acciones a realizar en cuanto se detecte el incidente y la respuesta al mismo para mitigar al máximo su impacto.

B. Propósito

Gestionar adecuadamente todos los incidentes de seguridad de la información reportados en la Municipalidad de Montes de Oro dando cumplimiento a los procedimientos establecidos.

C. Alcance

Esta política aplica para todos los colaboradores de la Municipalidad de Montes de Oro que detecten un evento o incidente de seguridad de la información el cual deben reportar.

D. Aplicación

A. Responsabilidades y procedimientos.

Para establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información hay que tener en cuenta lo siguiente:

- Establecer las responsabilidades en la gestión de incidentes de seguridad digital dentro del MEN.
- Definir el procedimiento de atención de incidentes de seguridad de la información del MEN.
- Dar un tratamiento adecuado a todos los incidentes de seguridad de la información reportados en el MEN.
- Realizar sensibilización a todos los colaboradores y terceros sobre incidentes de seguridad de la información.

B. Reporte de eventos de seguridad de la información.

- Informar sobre los eventos de seguridad de la información a través de los canales de gestión apropiados, tan pronto como sea posible.
- Reportar de forma inmediata de acuerdo con el procedimiento previsto los eventos, incidentes o debilidades en cuanto a la seguridad de la información que identifiquen o se presenten.

C. Evaluación de eventos de seguridad de la información.

- Evaluar los eventos de seguridad de la información y decidir si se van a clasificar.
- Evaluar cada evento o incidente de seguridad de la información presentado en la Municipalidad de Montes de Oro, con el fin de poder determinar clasificación y priorización.
- Registrar los resultados de la evaluación y la decisión para referencia y verificación futuras.

D. Respuesta a incidentes de seguridad de la información.

Responder a los incidentes de seguridad de la información que se presenten en la Municipalidad de Montes de Oro.

La respuesta debe incluir lo siguiente:

- Recolectar evidencia lo más pronto posible después de que ocurra el incidente.
- Llevar a cabo análisis forense de seguridad de la información, según se requiera.
- Llevar el asunto a una instancia superior, según se requiera.
- Asegurarse de que todas las actividades de respuesta involucradas se registren adecuadamente para análisis posterior.
- Tratar las debilidades de seguridad de información que se encontraron que causan o contribuyen al incidente.
- Una vez que el incidente se haya tratado lo suficiente, cerrarlo formalmente y hacer un registro de esto.

E. Aprendizaje obtenido de los incidentes de seguridad de la información.

- Usar el conocimiento adquirido al analizar y resolver incidentes de seguridad de la información para reducir la posibilidad o el impacto de incidentes futuros.
- Documentar todos los incidentes de seguridad de la información reportados en la Municipalidad de Montes de Oro.
- Llevar una bitácora de los incidentes de seguridad de la información reportados y atendidos en la Municipalidad de Montes de Oro.

F. Recolección de evidencia.

- Definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
- Desarrollar y seguir procedimientos internos cuando se trata con evidencia para propósitos de acciones legales y disciplinarias en la Municipalidad de Montes de Oro.

3.7 Control de activos de información

A. Descripción General

La Municipalidad de Montes de Oro comprende la importancia de una adecuada gestión de los activos, por lo cual tener un inventario y conocer la responsabilidad de los activos de información es parte esencial del sistema de gestión de Seguridad de la Información de la entidad, dado que a través de éste se conoce cuántos activos tiene la entidad, sus propietarios y los responsables de los mismos.

B. Propósito

Definir las políticas para la gestión de los activos de la institución que incluye el inventario y la responsabilidad sobre los activos de información.

C. Alcance

Aplica para todos los colaboradores de la Municipalidad de Montes de Oro que tenga acceso a los recursos y activos de información durante su ciclo de vida (creación, distribución, transmisión, almacenamiento, eliminación), y a los activos de información en todas sus formas (digital, impresa, escrita, y verbal).

D. Aplicación

A. Inventario de Activos.

1. Inventario de Activos.

Se deben identificar los activos asociados con la información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.

2. Propiedad de los Activos.

Los activos de información que hacen parte del inventario deben tener un propietario o responsable, de acuerdo con la asignación de activos fijos en el caso del hardware y de la información de acuerdo con el rol desempeñado en la entidad.

3. Encargado de inventarios de activos de información.

Responsable encargado de generar, mantener y actualizar el inventario de los activos de la entidad, así como la asignación indicando los responsables de la custodia de dichos activos.

4. Personal de la Municipalidad de Montes de Oro.

Responsable encargado de garantizar la integridad, confidencialidad y disponibilidad del inventario de activos que este bajo su custodia.

5. Uso Aceptable de los Activos.

Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.

6. Devolución de los Activos.

Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.

7. Etiquetado de Activos.

Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la entidad.

8. Eliminación de Activos.

La eliminación o destrucción de los activos de información, sean estos documentos en papel, bienes muebles (equipos, computadores, notebook, u otros similares), deberá efectuarse de acuerdo con la normatividad vigente.

3.8 Detección de intrusión

A. Descripción General

Un Sistema de Detección de Intrusos es un programa utilizado para analizar la detección de supuestos intrusos en la red o un computador, basado en sensores virtuales, permiten monitorear el tráfico de la red, permitiendo así evitar posibles ataques.

B. Propósito

Es un proceso de auditoría de la información del sistema de la red o de un computador, logrando a través de una configuración y de una base de datos prevenir y detectar posibles ataques de intrusos.

C. Alcance

Esta política aplica para todos los colaboradores de la Municipalidad de Montes de Oro que detecten un evento o incidente de seguridad de la información.

D. Aplicación

El proceso de detección de intrusos, se lo define de la siguiente manera:

- Una base de datos con una recopilación de ataques anteriores.
- Un sistema actual debidamente configurado.
- Estado actual, referente en términos de comunicación y procesos.

Además, el Sistema de Detección de Intrusos posee diferentes tipos los cuales se especificarán a continuación:

- Sistema de Detección de Intrusos basados en Host, estos solo procesan determinadas actividades de los usuarios o computadoras.
- Sistema de Detección de Intrusos basados en Red, monitorean generalmente algún punto de la red, en busca de intrusos. Bien ubicados en la red, pueden ser una alternativa excelente para la prevención de los intrusos y un bajo impacto en la red al abarcar grandes redes.
- Sistema de Detección de Intrusos basados en Log, revisa los archivos de Logs en busca de posibles intrusos, se caracteriza por su precisión y completitud.

Todos estos Sistemas de Detección serán usados por el Departamento de Tecnologías de Información y el mismo departamento tomara las medidas necesarias para controlar la intrusión.

3.9 Acceso a la red

A. Descripción General

Diseñar una política para garantizar que la red informática esté protegida de cualquier acto o proceso que pueda violar su seguridad.

B. Propósito

Fortalecer la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte de la Municipalidad de Montes de Oro.

C. Alcance

Esta política aplica para todas las redes, los servicios de red y los controles utilizados para proteger la información en la transferencia de información de la Municipalidad de Montes de Oro.

D. Aplicación

A. Controles de Redes.

- Gestionar y controlar las redes para proteger la información en sistemas y aplicaciones.
- Establecer los controles lógicos para el acceso a los diferentes recursos informáticos, con el fin de mantener los niveles de seguridad apropiados.
- Proporcionar a los colaboradores y terceros todos los recursos tecnológicos de conectividad necesarios para que puedan desempeñar las funciones y actividades laborales.

- Monitorear la funcionalidad de las redes a través del uso de analizadores de red.
- No es permitido conectar a las estaciones de trabajo o a los puntos de acceso de la red corporativa, elementos de red (tales como switches, enrutadores, módems, etc.) que no sean autorizados por el Departamento de Tecnologías de Información.

B. Seguridad de los servicios de red.

- Dar el acceso a internet exclusivamente a través de la red establecida para ello, es decir, por medio del sistema de seguridad con Firewall incorporado en la misma.
- Utilizar el acceso a la red, Internet, exclusivamente para el desarrollo de sus actividades propias de las funciones desempeñadas en la Municipalidad de Montes de Oro.
- El acceso de los colaboradores a la red debe realizarse a través de la red inalámbrica definida como (MuniMonOro) o mediante la red cableada.
- Conectarse única y exclusivamente a la red inalámbrica (InviMonOro) de la Municipalidad de Montes de Oro a internet sin la necesidad de algún tipo de cableado. La red inalámbrica de invitados le permitirá utilizar los servicios de internet, en las zonas de cobertura de la Municipalidad de Montes de Oro.
- Los usuarios que accedan a través de la red invitados no tendrán acceso a los servicios, sistemas de información, etc., de la Municipalidad de Montes de Oro ni a ningún recurso de uso privado.

C. Separación en las redes.

- Establecer un esquema de segregación de redes, con el fin de controlar el acceso a los diferentes segmentos de red y buscar que

se preserve la confidencialidad, integridad y disponibilidad de la información de la Municipalidad de Montes de Oro.

- Establecer parámetros técnicos para la conexión segura de la red con los servicios de red.
- Establecer mecanismos de autenticación seguros para el acceso a la red.
- Separar las redes inalámbricas públicas de las redes internas, para preservar los principios de la seguridad de la información.

3.10 Acceso físico

A. Descripción General

Lo definido en la presente política aplica para el control de acceso físico a las áreas seguras dentro de las cuales se encuentran el centro de datos, centros de cableado, áreas de tesorería, archivo, áreas de recepción y entrega de correspondencia y controles de acceso adecuados para la protección de la información de la Municipalidad de Montes de Oro.

B. Propósito

Prevenir el acceso físico no autorizado, el daño y la interferencia a la información a las instalaciones de procesamiento de información de la Municipalidad de Montes de Oro.

C. Alcance

Aplica para todos los colaboradores de la Municipalidad de Montes de Oro que tengan acceso a diferentes áreas de la institución, esto con el fin de controlar el acceso físico a las áreas donde se encuentras los centros de datos.

D. Aplicación

A. Perímetro de seguridad física.

- El perímetro de seguridad de las instalaciones de la Municipalidad de Montes de Oro o de las áreas seguras debe ser físicamente sólido (no deben existir aberturas en el perímetro o áreas donde pueda producirse fácilmente una irrupción). Las paredes externas del área deben ser de construcción sólida y todas las puertas que comunican con el exterior deben ser adecuadamente protegidas contra accesos no autorizados, por ejemplo, mediante mecanismos de control, vallas, alarmas, cerraduras, etc.
- Verificar que las puertas y ventanas de las áreas seguras estén cerradas con llave cuando no hay supervisión o están desocupadas.
- El perímetro de seguridad de las áreas seguras debe contar con vigilancia mediante CCTV, contar con sistemas de control de acceso y debe ser monitoreado por el personal de seguridad de la institución.

- Todas las puertas de emergencia de un perímetro de áreas seguras deben tener alarma.

B. Controles de acceso físico.

- Todos los puntos de acceso a las instalaciones físicas deberán tener un área de recepción con vigilancia u otro medio para controlar el acceso físico a las instalaciones y debe estar documentado.
- El personal de seguridad debe establecer mecanismos para inspeccionar y examinar los bolsos, cajas, etc. de los colaboradores o visitantes que ingresen y salen de las instalaciones de la Municipalidad de Montes de Oro.
- Registrar en una bitácora o sistema de información el ingreso y retiro de todo equipo de cómputo, servidores, equipos activos de red o cualquier equipo diferente a smartphone; en caso de que estos equipos sean propiedad del Ministerio deberán contar con autorización expresa según sea el caso y de acuerdo con los procedimientos establecidos para tal fin.
- Las áreas seguras se deberían proteger mediante controles de entrada, apropiados para asegurar que solamente se permite el acceso a personal autorizado
- Se debe autorizar el acceso al centro de cómputo, centros de cableado y centro de servidores ya que es restringido este acceso y solo debería ingresar el personal autorizado. Adicionalmente, se debe realizar el monitoreo correspondiente a estos accesos.

C. Seguridad de oficinas, recintos e instalaciones.

- Borrar la información escrita en los tableros o pizarras al finalizar las reuniones de trabajo. Igualmente, no se deben dejar documentos o notas escritas en los espacios al finalizar las reuniones.
- Garantizar que los visitantes se encuentren acompañados de un colaborador de la Municipalidad de Montes de Oro, cuando se encuentren en las oficinas o áreas seguras donde se maneje información.
- Asegurar que los visitantes que requieran permanecer en las oficinas de la Municipalidad de Montes de Oro por periodos superiores a dos días sean presentados al personal de oficina donde permanecerán.
- Portar su carné en un lugar visible mientras permanezca dentro de las instalaciones de la institución.
- En ninguna circunstancia, se debe fumar, comer o beber en las áreas seguras.
- Verificar que no se toman fotografías o grabación de video, en áreas de procesamiento de información o donde se encuentren activos de información que comprometan la seguridad o la imagen de la Municipalidad de Montes de Oro, a menos que esté autorizado.
- Verificar que las instalaciones estén configuradas para evitar que las actividades o información confidenciales sean visibles y audibles desde el exterior.

3.11 Dispositivos Móviles

A. Descripción General

Evitar que los dispositivos móviles sean causa de infección y/o distribución de código malicioso.
Además de prevenir que éstos sean el origen de accesos no autorizados a las redes o recursos privados de la Municipalidad de Montes de Oro.

B. Propósito

Se debe adoptar una política y unas medidas de seguridad de soporte para gestionar los riesgos introducidos por el uso de dispositivos móviles.

C. Alcance

Se aplica a todos los usuarios en la Municipalidad de Montes de Oro, incluyendo las empresas que presten servicios a la entidad.

D. Aplicación

- Llevar un registro y control de todos los dispositivos móviles (portátiles, tabletas y teléfonos móviles) que posee la Municipalidad de Montes de Oro. (Entrega y recibido de los dispositivos) y hacer firmar por

parte del servidores públicos y contratistas el compromiso de cumplimiento de controles.

- Definir un procedimiento formal de salida de dispositivos de las instalaciones, donde se especifique, entre otras cosas, que el uso de los equipos portátiles de propiedad de la Municipalidad de Montes de Oro, fuera de las instalaciones, únicamente se permitirá a usuarios autorizados mediante una orden de salida, la cual debe tener el visto bueno del jefe inmediato con firma autorizada para este fin.
- Autorizar la salida de equipos de dispositivos móviles para la ejecución de actividades fuera de las instalaciones de la Municipalidad de Montes de Oro.
- No permitir la salida de equipos de escritorio para la ejecución de cualquier actividad fuera de las instalaciones de la Municipalidad de Montes de Oro. Cuando por alguna excepción se requiera la salida de un equipo de escritorio deberá tener la autorización previa del Departamento de Tecnologías de Información, con el fin de verificar que tipo de información se encuentra almacenada en el equipo.
- Contar con un sistema de autenticación, como un patrón, código de desbloqueo o una clave, para todos los dispositivos móviles, como celulares, que almacenen información de la institución.
- Mantener apagado el bluetooth o cualquier otra tecnología inalámbrica que exista o llegara a existir.
- No instalar ni configurar en los servicios ni en la infraestructura tecnológica de la institución
- Derecho a revisar la utilización del dispositivo móvil ante cualquier indicio de un uso inapropiado del mismo, inspeccionarlo o disponer de el de cualquier forma, dado que el dispositivo móvil como la información almacenada es propiedad de la Municipalidad de Montes de Oro.

3.12 Acceso remoto

A. Descripción General

Garantizar la seguridad de la información cuando se accede remotamente a los sistemas de información de la Municipalidad de Montes de Oro.

B. Propósito

La Municipalidad Montes de Oro debe implementar políticas y medidas de seguridad para la operación de la información a través del acceso remoto.

C. Alcance

Debe ser cumplida por todos los colaboradores en la Municipalidad de Montes de Oro y también por los colaboradores de la misma institución que presten servicios desde su domicilio.

D. Aplicación

- Contar con las aprobaciones requeridas para establecer conexión remota a los dispositivos de la plataforma tecnológica de la Municipalidad de Montes de Oro.

- Establecer conexiones remotas únicamente a través de las conexiones seguras y utilizar computadores en sitios confiables (Ej. Casa) y, en ninguna circunstancia, en computadores públicos, de hoteles o cafés internet, entre otros.
- Configurar las conexiones remotas a los servicios tecnológicos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores asignadas dentro de la Municipalidad de Montes de Oro.
- El colaborador que solicite el acceso remoto es responsable del uso adecuado del mismo.

3.13 Uso del Antivirus

A. Descripción General

La Municipalidad de Montes de Oro está en la obligación de proteger la información que le pertenece y que se encuentra en su custodia, de instrucciones maliciosas. Así, con el fin de mantenerse alerta ante la presencia de virus, y de poder responder adecuadamente para prevenirlos o administrar sus consecuencias, es que se aprueban estas políticas de uso de antivirus.

B. Propósito

Establecer los requerimientos que en materia de antivirus deben ser satisfechos, para todos los equipos computacionales conectados de manera lógica o física, a los sistemas informáticos o redes de la Municipalidad de Montes de Oro, a fin de prevenir y detectar de manera efectiva algún problema.

C. Alcance

Estas políticas son aplicables a todos los usuarios de equipos computacionales que hayan de ser conectados a los sistemas informáticos de la Municipalidad de Montes de Oro.

D. Aplicación

A. Uso del Antivirus y Prevención de Infestación.

1.Responsabilidad del personal con respecto a la aplicación del antivirus aprobada por la institución.

Todos los colaboradores deben tener instalada y efectivamente activa, en el equipo computacional que utiliza la Municipalidad de Montes de Oro, la aplicación antivirus formalmente aprobada, corriendo en su última versión, antes de proceder a conectarse a los sistemas de la Institución. A menos que cuente con autorización expresa y por escrito válidamente emitida para tales efectos, ningún usuario debe por su propia cuenta y por ninguna razón, deshabilitar las aplicaciones de antivirus instaladas en los equipos de la Institución. Toda instalación o desinstalación de las aplicaciones de antivirus, será llevada a cabo únicamente por personal del Departamento de Tecnologías de Información.

2. Prohibición del personal de tratar de eliminar una instrucción maliciosa por sus propios medios.

Los colaboradores, no deben bajo ninguna circunstancia tratar de eliminar instrucciones maliciosas de los equipos o sistemas conectados a la red de la Municipalidad de Montes de Oro, por sus

propios medios. Ante la mera sospecha de la existencia de una instrucción maliciosa, el usuario debe proceder inmediatamente a hacer uso de los canales formalmente aprobados para hacer el respectivo reporte, ante el Departamento de Tecnologías de Información.

3. Instalación y actualización de software antivirus en equipo aprobado.

Solamente el Departamento de Tecnologías de Información, procederá a instalar el software antivirus que la Institución haya previamente aprobado y que cuente con su respectiva licencia. Este software se instalará únicamente en aquellos equipos computacionales que haya sido, a su vez, previamente autorizados.

4. Prohibición de utilizar cualquier software no licenciado no autorizado por la Municipalidad de Montes de Oro.

A menos que expresamente se estipule lo contrario, está absolutamente prohibida la instalación y utilización de cualquier tipo de software no licenciado o no autorizado, en los equipos o sistemas conectados a la red de la Institución.

5. Archivos y software proveniente de fuentes desconocidas.

No deben ejecutarse archivos ni software que provengan de fuentes desconocidas en los equipos o sistemas conectados a la red de la Municipalidad de Montes de Oro. Siempre que se tenga motivo suficiente y fundamentado para creer que un archivo o software de fuente desconocida pueda contener información de importancia para la Municipalidad de Montes de Oro, debe contactarse inmediatamente al

Departamento de Tecnologías de Información, para que este pueda accederla en un ambiente controlado.

B. Escogencia y administración de la plataforma Antivirus.

1. Escogencia y aprobación de al menos una aplicación antivirus Para la Municipalidad de Montes de Oro.

Para el desarrollo, adquisición, modificación, y actualización de sus sistemas, se debe escoger y estandarizar el uso de al menos una aplicación de antivirus que provea la protección contra instrucciones malignas que la Institución necesita. Esta aplicación debe mantenerse permanentemente actualizada y licenciada corporativamente, para todas las redes, sistemas y estaciones de trabajo, tomando en cuenta las expectativas de crecimiento de la Institución. Asimismo, debe proporcionarse capacitación suficiente y constante a quienes administren la plataforma escogida.

2. Administración de la plataforma de antivirus.

Corresponderá al Departamento de Tecnologías de Información la administración de la plataforma de antivirus, de modo que la misma se mantenga funcionando óptimamente y permanentemente actualizada. El personal del Departamento de Informática tendrá la responsabilidad de mantenerse capacitado en la herramienta, de manera que pueda sacarle el mejor provecho en beneficio de la institución.

3. Revisión periódica de los equipos y sistemas conectados a la red de la Municipalidad de Montes de Oro a efectos de controlar instrucciones maliciosas.

En la sana administración de los sistemas y a fin de evitar y controlar instrucciones maliciosas, el Departamento de Informática debe llevar a

cabo revisiones periódicas en sus sistemas y equipos, dirigidas a garantizar que los mismos se encuentran libres de códigos malignos, así como asegurar que los usuarios posean instalado el software de antivirus aprobado por la Institución.

4. Recuperación frente a virus.

Se deben contemplar entre otras cosas, provisiones para la recuperación rápida y eficiente ante ataques por virus, incluyendo protección de la información de la Institución.

5. Controles contra puertas ocultas y códigos troyanos.

Se deben establecer controles dirigidos a procurar evitar la instalación de puertas ocultas y código troyano en los sistemas de la Municipalidad de Montes de Oro.

Así, los controles mínimos que deben aplicarse serán:

- Adquirir programas únicamente de proveedores acreditados.
- Adquirir programas en código fuente de manera que el mismo pueda ser verificado.
- Utilizar productos previamente evaluados.
- Examinar todo el código fuente antes de pasar un programa a producción.
- Controlar el acceso y las modificaciones al código una vez instalado el mismo.
- Emplear personal de probada confiabilidad para trabajar en los sistemas críticos.

3.14 Mantenimientos de Activos.

A. Descripción General

Lo definido en la presente política aplica para el mantenimiento de los activos y asegurar una mejor protección para la información de la Municipalidad de Montes de Oro.

B. Propósito

Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.

C. Alcance

Aplica para todos los colaboradores de la Municipalidad de Montes de Oro del Departamento de Tecnologías de Información.

D. Aplicación

- Asegurar que se les efectúe mantenimiento a los equipos adecuadamente con el objeto de garantizar su disponibilidad e integridad continua.

- Asegurar el correcto funcionamiento de los equipos de cómputo, concretando tiempos de mantenimiento de los equipos con el Departamento de Tecnologías de Información y con los colaboradores.
- Sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
- Se deben mantener registros de todas las fallas supuestas o reales y de todo el mantenimiento preventivo y correctivo.
- Contemplar un mantenimiento preventivo a los servidores del centro de cómputo trimestralmente.

3.15 Gestión de Actualizaciones

A. Descripción General

Todo software es susceptible de necesitar actualizaciones por motivos de seguridad, esto incluye los equipos electrónicos, los sistemas operativos y aplicaciones informáticas e incluso los propios programas antivirus. Los fabricantes de software lanzan actualizaciones y parches que mejoran y añaden nuevas funcionalidades, o que corrigen errores y agujeros de seguridad.

B. Propósito

Revisar la existencia de actualizaciones y parches de seguridad para nuestro software y elaborar procedimientos que permitan que tales actualizaciones y parches sean instalados en nuestros equipos de forma segura y controlada.

C. Alcance

Se aplica a todos los colaboradores con equipos computacionales de la Municipalidad de Montes de Oro y al Departamento de Tecnologías de Información.

D. Aplicación

1. Determinar el software qué debe ser actualizado.

Tendremos que realizar un inventario de todo el software instalado, ya que pueden descubrirse errores o mejoras de funcionalidad. Para corregir dichos errores y garantizar un comportamiento óptimo debemos instalar, en cuando tengamos conocimiento de ellos, las correspondientes actualizaciones y parches de seguridad.

2. Determinar cuándo y qué actualizaciones instalar.

El departamento de Tecnologías de Información determinará el momento en que ejecutar las actualizaciones para no interferir con las operaciones de la empresa. Aunque los principales programas comerciales disponen de funcionalidades de actualización automática, cabe la posibilidad de que tengamos software instalado que no disponga de estas opciones de actualización.

Antes de su instalación el Departamento de Tecnologías considerará la utilidad de las nuevas mejoras, así como los requisitos necesarios.

3. Probar las actualizaciones.

Siempre debemos instalar actualizaciones provenientes de fuentes confiables. No obstante, se debe sopesar la necesidad de disponer de un entorno de pruebas o preproducción donde instalar y probar las

actualizaciones, de este modo podremos verificar que su funcionamiento es el esperado.

4. Deshacer los cambios.

Antes de aceptar la instalación de una actualización, se debe considerar la forma de deshacer los cambios realizados. Así si el comportamiento del software actualizado no responde a lo esperado podremos volver a la situación anterior. Siempre es recomendable disponer antes de cualquier cambio de copias de seguridad recientes localizadas y probadas.

5. Herramientas de diagnóstico y actualización.

Existen herramientas que revisan si el software de nuestros equipos está actualizado o no. Una vez detectadas las actualizaciones pendientes, podemos proceder a su instalación en todos los equipos de manera centralizada. Esto puede ser útil en entornos con muchos equipos en los que queremos que el software instalado sea homogéneo y esté especialmente controlado.

6. Registro de actualizaciones.

Realizaremos un registro de las actualizaciones que se han instalado en nuestros sistemas. De esta forma podremos tener en todo momento un conocimiento exhaustivo del software operativo en nuestros equipos.