

RESOLUCIÓN DE GERENCIA MUNICIPAL N° 656- 2022-GM-MVES.

Villa el Salvador, 16 de diciembre del 2022.

VISTOS; Los Informes N° 353-2022-OAJ/MVES de fecha 16 de diciembre del 2022 de la Oficina de Asesoría Jurídica; Informe N° 0169-2022-UDT-OGA/MVES, de fecha 28 de noviembre de 2022, de la Subgerencia de la Unidad de Desarrollo Tecnológico; sobre Revisión y Aprobación de Política de Seguridad de la Información de la Municipalidad Distrital de Villa El Salvador y;

CONSIDERANDO;

Que, el artículo 194° de la Constitución Política del Perú, establece que: "Las Municipalidades provinciales y distritales son los órganos de gobierno local. Tienen autonomía política, económica y administrativa en los asuntos de su competencia (...)", lo cual concuerda con el artículo II del Título Preliminar de la Ley N° 27972, Ley Orgánica de Municipalidades, que establece que los gobiernos locales gozan de autonomía política, económica y administrativa, en los asuntos de su competencia; siendo que esta autonomía radica en la facultad de ejercer actos de gobierno, administrativos y de administración, con sujeción al ordenamiento jurídico;

Que, por el artículo 1° y el artículo 2° del Decreto Supremo N°004-2013-PCM, se decreta lo siguiente: **Artículo 1°.- Aprobación de la Política Nacional de Modernización de la Gestión Pública.** Apruébese la Política Nacional de Modernización de la Gestión Pública, la cual forma parte integrante del presente Decreto Supremo como Anexo, siendo el principal instrumento orientador de la modernización de la gestión pública en el Perú, que establecerá la visión, los principios y lineamientos para una actuación coherente y eficaz del sector público, al servicio de los ciudadanos y el desarrollo del país; **Artículo 2°.- Ámbito de aplicación.** La Política Nacional de Modernización de la Gestión Pública es de aplicación a las Entidades de la Administración Pública, que se señalan a continuación: (...) 3. Los Gobiernos Locales;

Que, Así mismo, subnumeral 2.2. del numeral 2 del Anexo del Decreto Supremo N°004-2013-PCM, el cual indica que: 2. Fundamentos de la política: visión, alcance, objetivo y principios (...)2.2. Alcance de la política Modernizar la gestión pública es una responsabilidad de todas las autoridades, funcionarios y servidores del Estado en cada uno de sus organismos y niveles de gobierno. En ese sentido, cualquier esfuerzo que apunte a elevar los niveles de desempeño de las entidades del Estado a favor de los ciudadanos, debe involucrar a los diversos sectores y niveles de gobierno. Por lo tanto, la modernización de la gestión pública es una política de Estado que alcanza a todas las entidades públicas que lo conforman, sin afectar los niveles de autonomía que les confiere la ley. Compromete al Poder Ejecutivo, organismos autónomos, gobiernos descentralizados, instituciones políticas y la sociedad civil, a través de sus distintas organizaciones."

Que, la Resolución Ministerial N° 004-2016-PCM, en su artículo 1° aprueba "(...) el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información Requisitos. 2da. Edición", en todas las entidades integrantes del Sistema Nacional de Informática; con la finalidad de coadyuvar con la infraestructura de Gobierno Electrónico, por considerar a la seguridad de la información como un componente crucial para dicho objetivo;

Que, en los artículos 2°, 3°, y 4° de la Ley N°27658, Ley Marco de Modernización de la Gestión del Estado, se establece que: "**Artículo 2.- Objeto de la ley** La presente Ley tiene por objeto establecer los principios y la base legal para iniciar el proceso de modernización de la gestión del Estado, en todas sus instituciones e instancias." "**Artículo 3.- Alcance de la ley** "La presente Ley es de aplicación en todas las dependencias de la Administración Pública a nivel nacional."

RESOLUCIÓN DE GERENCIA MUNICIPAL N° 656- 2022-GM-MVES.

Villa el Salvador, 16 de diciembre del 2022.

“Artículo 4.- Finalidad del proceso de modernización de la gestión del Estado; El proceso de modernización de la gestión del Estado tiene como finalidad fundamental la obtención de mayores niveles de eficiencia del aparato estatal, de manera que se logre una mejor atención a la ciudadanía, priorizando y optimizando el uso de los recursos públicos. El objetivo es alcanzar un Estado: a) Al servicio de la ciudadanía. b) Con canales efectivos de participación ciudadana. c) Descentralizado y desconcentrado. d) Transparente en su gestión. e) Con servidores públicos calificados y adecuadamente remunerados. f) Fiscalmente equilibrado”;

Que, el artículo 3° de la Ley N°29733, Ley de Protección de Datos Personales, establece lo siguiente: **“Artículo 3. Ámbito de aplicación** La presente Ley es de aplicación a los datos personales contenidos o destinados a ser contenidos en bancos de datos personales de administración pública y de administración privada, cuyo tratamiento se realiza en el territorio nacional. Son objeto de especial protección los datos sensibles. (...);”

Que, el artículo 1° del Decreto Legislativo N°1412, Decreto Legislativo que Aprueba la Ley de Gobierno Digital, establece que: **“Artículo 1.- Objeto** “La presente Ley tiene por objeto establecer el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno.;

Que, los numerales 6.1 y 6.2 del artículo 6° y el numeral 7.1 del artículo 7° del precitado Decreto Legislativo, señala en referencia al Gobierno Digital, que: **“Artículo 6.- Gobierno Digital 6.1.** El gobierno digital es el uso estratégico de las tecnologías digitales y datos en la Administración Pública para la creación de valor público. Se sustenta en un ecosistema compuesto por actores del sector público, ciudadanos y otros interesados, quienes apoyan en la implementación de iniciativas y acciones de diseño, creación de servicios digitales y contenidos, asegurando el pleno respeto de los derechos de los ciudadanos y personas en general en el entorno digital. **6.2.** Comprende el conjunto de principios, políticas, normas, procedimientos, técnicas e instrumentos utilizados por las entidades de la Administración Pública en la gobernanza, gestión e implementación de tecnologías digitales para la digitalización de procesos, datos, contenidos y servicios digitales de valor para los ciudadanos;” **“Artículo 7.- Objetivos del Gobierno Digital** Los objetivos del gobierno digital son: **7.1** Normar las actividades de gobernanza, gestión e implementación en materia de tecnologías digitales, identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos. (...);”

Que, el artículo 30° del Decreto Legislativo N°1412, Decreto Legislativo que Aprueba la Ley de Gobierno Digital, establece que: **“Artículo 30°.- De la Seguridad Digital** La seguridad digital es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas;”

RESOLUCIÓN DE GERENCIA MUNICIPAL N° 656- 2022-GM-MVES.

Villa el Salvador, 16 de diciembre del 2022.

Que, Con Resolución N°439-2021-GM-MVES se aprueba conformar el Comité de Gobierno Digital de la Municipalidad de Villa El Salvador, por el cual se resuelve en su artículo Primero que: **Artículo Primero.** - CONFORMAR el Comité de Gobierno Digital de la Municipalidad Distrital de Villa El Salvador, el mismo que estará integrado por los siguientes miembros: **En representación del Titular de la Entidad, El Gerente Municipal.; El Gerente Municipal, Como Líder de Gobierno Digital.**

Que, el numeral 36.1 y 36.4 del artículo 36° de la Ordenanza N° 441-MVES, Ordenanza que modifica la Estructura Orgánica de la Municipalidad Distrital de Villa El Salvador y el Reglamento de Organización y Funciones (ROF), con enfoque de Gestión de Resultados de la Municipalidad Distrital de Villa el Salvador aprobado con Ordenanza N° 369-MVES, indica que la Unidad de Desarrollo Tecnológico tiene entre sus competencias respecto a la función de planeamiento y función normativa y reguladora, que: "36.1 Diseñar el Plan de Contingencias Informático, el Plan de Seguridad de la Información, y otros planes que sean de su competencia." (...) "36.4 Proponer proyectos de normas Municipales en materia de su competencia, para la mejora de la gestión."

Que, Con Resolución de Alcaldía N°164-2021-ALC/MVES, se designa al Gerente Municipal en el Cargo de Líder de Gobierno Digital de la Municipalidad Distrital de Villa El Salvador, quien estará a cargo "de coordinar objetivos, acciones y medidas para la transformación digital y despliegue del Gobierno Digital a nivel institucional, conforme a las políticas y directrices emitidos por la Presidencia del Consejo de Ministros, (...);"

Que, Mediante Informe N° 0169-2022-UDT-OGA/MVES de fecha 28 de noviembre del 2022, la Subgerencia de la Unidad de Desarrollo Tecnológico remite a la Gerencia Municipal, la Revisión y Aprobación de Política de Seguridad de la Información de la Municipalidad Distrital de Villa el Salvador, esto en cumplimiento a lo solicitado por el órgano de Control Institucional, correspondiente a la Situación Adversa N° 05 del Informe de orientación de Oficio N° 20410-2021-CG/GRILIM-SOO "Implementación, funcionalidad y Políticas de Seguridad del Sistema de Recaudación y Sistema de Administración Financiera de la MVES".

Que, mediante Informe N° 353-2022-OAJ/MVES, de fecha 16 de diciembre 2022, la Gerencia de Asesoría Jurídica opina que es legalmente procedente la Aprobación mediante Resolución de Gerencia Municipal el "Plan de Política de Seguridad de la Información, con el fin de atender la Situación Adversa N° 05 correspondiente al Informe de Orientación de Oficio N° 20410-2021—CG/GRLIM-SOO; la aprobación de dicho Plan se aprobará mediante Resolución de Gerencia Municipal, ello en conformidad con lo resuelto en el artículo 1° y 2° de la Resolución N° 439-2021-GM-MVES; y del numeral 14.2 Y 14.3 del artículo 14° de la Ordenanza N° 441-MVES;

Que, conforme a las atribuciones conferidas en el artículo 27° de la Ley N° 27972 - Ley Orgánica de Municipalidades y al amparo del numeral 14.9 y 14.12 del artículo 14° de la Ordenanza N° 441-MVES, que aprueba el Texto Íntegro del Reglamento de Organización y Funciones -ROF con enfoque de gestión de resultados de la Municipalidad Distrital de Villa El Salvador, aprobado mediante Ordenanza N° 369-MVES; que señala: "14.9) Emitir Resoluciones de Gerencia Municipal, (...), y "14.12) Dirigir los Procesos de Modernización y fortalecimiento Institucional acorde con las Políticas Nacionales y los objetivos de estratégicos de desarrollo local";



CENTRAL TELEFÓNICA 319-2530
www.munives.gob.pe

RESOLUCIÓN DE GERENCIA MUNICIPAL N° 656- 2022-GM-MVES.

Villa el Salvador, 16 de diciembre del 2022.

SE RESUELVE:

ARTICULO PRIMERO. – APROBAR; el Plan de Política de Seguridad de la Información de la Municipalidad Distrital de Villa El Salvador; según lo expuesto en la parte considerativa de la presente Resolución.

ARTICULO SEGUNDO.- ENCARGAR al Subgerente de la Unidad de Desarrollo Tecnológico de la Entidad el desarrollo, ejecución y cumplimiento del Plan de Política Seguridad de la Información; el mismo que deberá ejecutarse en cumplimiento de la normatividad legal vigente; bajo responsabilidad.

ARTICULO TERCERO. - ENCARGAR a la Unidad de Desarrollo Tecnológico, efectuar la publicación de la presente Resolución de Gerencia Municipal, en el Portal Institucional de la Municipalidad Distrital de Villa El Salvador (www.munives.gob.pe).

REGÍSTRESE, COMUNÍQUESE Y CÚMPLASE.

MUNICIPALIDAD DE VILLA EL SALVADOR
GERENCIA MUNICIPAL


JOSÉ LUIS ESPICHÁN PÉREZ
GERENTE





MUNICIPALIDAD DE VILLA EL SALVADOR
OFICINA DE ASESORIA JURIDICA

INFORME N° 353-2022-OAJ/MVES

A : **Abog. José Luis Espichan Pérez**
Gerente Municipal

DE : **Abg. Shirlet Marley Castro Gonzáles**
Gerente de la Oficina de Asesoría Jurídica

ASUNTO : Opinión Legal sobre Revisión y Aprobación de Política de Seguridad de la Información de la Municipalidad Distrital de Villa El Salvador.

REF. : Memorando N° 1219-2022-GM/MVES

FECHA : Villa el Salvador, 15 de diciembre del 2022



Por medio del presente, y en atención al documento de la referencia, la Oficina de la Gerencia Municipal solicita se emita opinión legal relacionada con el asunto del rubro, procedemos a la emisión del mismo, en los términos siguientes:

I. ANTECEDENTES:

1. Memorandum N°1219-2022-GM/MVES de fecha 29 de noviembre del 2022, la Oficina de la Gerencia Municipal corre traslado a la Gerencia de la Oficina de Asesoría Jurídica, a fin emitir Opinión Legal respecto al instrumento legal para aprobar la Política de Seguridad de la Información de la Municipalidad Distrital de Villa El Salvador, ello al amparo del numeral 24.9 del artículo 24° de la Ordenanza N°441-MVES.
2. Informe N°0169-2022-UDT-OGA/MVES de fecha 25 de noviembre del 2022, la Subgerencia de la Unidad de Desarrollo Tecnológico remite a la Oficina de la Gerencia Municipal el Proyecto de Política de Seguridad de la Información de la Municipalidad Distrital de Villa El Salvador, para que la Gerencia de la Oficina de Asesoría Jurídica determine el instrumento legal a Utilizarse para su aprobación.
3. Memorando N°925-2022-GM/MVES de fecha 13 de setiembre del 2022, la Oficina de la Gerencia Municipal remite a la Subgerencia de la Unidad de Desarrollo Tecnológico, el "Reporte de Seguimiento de las acciones para el tratamiento de situaciones adversas resultantes de servicio de control simultaneo" del 01 al 31 de agosto del 2022", en solicitud de cumplir con la ejecución de los Planes de Acción de las Situaciones Adversas remitidas por el Órgano de Control Interno -OCI.
4. Informe N°0213-2021-UDT-OGA/MVES de fecha 23 de noviembre del 2021, la Subgerencia de la Unidad de Desarrollo Tecnológico remite a la Oficina General





**MUNICIPALIDAD DE VILLA EL SALVADOR
OFICINA DE ASESORIA JURIDICA**

de Administración el Plan de Acción para implementar la Situación Adversa N°05 correspondiente al Informe de Orientación de Oficio N°20410-2021-CG/GRLIM-SOO, en respuesta a la situación adversa N°05 entre otros, contenidas en el informe, por el que se señala que, *“la Entidad no cuenta con políticas de seguridad de la información aprobadas, careciendo de controles definidos para identificar las deficiencias en el diseño e implementación de los sistemas y el tratamiento de los riesgos y amenazas, afectando la protección de los activos de información”*.

5. Memorando Múltiple N°062-2021-OGA/MVES de fecha 17 de noviembre del 2021, la Oficina General de Administración, solicita a la Subgerencia de la Unidad de Desarrollo Tecnológico, que se remita el Plan de Acción de la Situación Adversa N°05 correspondiente a la “Comunicación del informe de Orientación de Oficio N°20110-2021-CG/GRLIM-SOO- Implementación, Funcionalidad y Política de Seguridad del Sistema de Recaudación y Sistema de Administración Financiera de la Municipalidad de Villa El Salvador”, el cual señala que esta Corporación Edil no cuenta con Políticas de Seguridad de la Información.

II. BASE LEGAL:

- ✓ Constitución Política del Perú.
- ✓ Ley N° 27972, Ley Orgánica de Municipalidades.
- ✓ Ley N° 27658, Ley Marco de Modernización de la Gestión Pública
- ✓ Ley N° 27815, Ley del Código de Ética de la Función Pública
- ✓ Ley N°29733, Ley de Protección de Datos Personales
- ✓ Decreto Legislativo N°1412, Decreto Legislativo que Aprueba la Ley de Gobierno Digital
- ✓ Decreto Supremo N°004-2013-PCM, aprueba la Política nacional de Modernización de la Gestión Pública.
- ✓ Resolución Ministerial N°246-2007-PCM, aprueba el uso obligatorio de la Norma Técnica Peruana “NTP-ISO/IEC 17799:2007 EDI. Tecnológica de la Información. Código de buenas practicas para la Gestión de la Seguridad de la Información.
- ✓ Directiva N°013-2022-CG/NORM “Servicio de Control Simultaneo”, aprobada con Resolución de Contraloría N°218-2022-CG.
- ✓ Resolución Ministerial N°004-2016-PCM,.
- ✓ Resolución de Contraloría 320-2006-CG, “Normas de Control Interno para las Entidades del Estado”.
- ✓ Ordenanza N° 441-MVES, Ordenanza que modifica la Estructura Orgánica de la Municipalidad Distrital de Villa El Salvador y el Reglamento de Organización y Funciones (ROF), con enfoque de Gestión de Resultados de la Municipalidad Distrital de Villa el Salvador aprobado con Ordenanza N° 369-MVES.

III. ANÁLISIS:

1. Que, el artículo 194° de la Constitución Política del Perú, artículo modificado por la Ley N° 30305, Ley de Reforma Constitucional, establece que:



MUNICIPALIDAD DE VILLA EL SALVADOR
OFICINA DE ASESORIA JURIDICA

82

- “Las municipalidades provinciales y distritales son los órganos de gobierno local. **Tienen autonomía política, económica y administrativa** en los asuntos de su competencia (...)”.
2. Que, el artículo II del Título Preliminar de la Ley N° 27972, Ley Orgánica de Municipalidades, establece que:

- “Los gobiernos locales gozan **de autonomía política, económica y administrativa, en los asuntos de su competencia**; siendo que esta autonomía radica en la facultad de ejercer actos de gobierno, administrativos y de administración, con sujeción al ordenamiento jurídico”.

3. Que, por el artículo 1° y el artículo 2° del Decreto Supremo N°004-2013-PCM, se decreta lo siguiente:

- **Artículo 1°.- Aprobación de la Política Nacional de Modernización de la Gestión Pública.**

Apruébese la Política Nacional de Modernización de la Gestión Pública, la cual forma parte integrante del presente Decreto Supremo como Anexo, siendo el principal instrumento orientador de la modernización de la gestión pública en el Perú, que establecerá la visión, los principios y lineamientos para una actuación coherente y eficaz del sector público, al servicio de los ciudadanos y el desarrollo del país

- **Artículo 2°.- Ámbito de aplicación.**

La Política Nacional de Modernización de la Gestión Pública es de aplicación a las Entidades de la Administración Pública, que se señalan a continuación:

(...)

3. Los Gobiernos Locales

4. Así mismo, subnumeral 2.2. del numeral 2 del Anexo del Decreto Supremo N°004-2013-PCM, el cual indica que:

- “2. Fundamentos de la política: visión, alcance, objetivo y principios

(...)

2.2. Alcance de la política Modernizar la gestión pública es una responsabilidad de todas las autoridades, funcionarios y servidores del Estado en cada uno de sus organismos y niveles de gobierno. En ese sentido, cualquier esfuerzo que apunte a elevar los niveles de





MUNICIPALIDAD DE VILLA EL SALVADOR
OFICINA DE ASESORIA JURIDICA

desempeño de las entidades del Estado a favor de los ciudadanos, debe involucrar a los diversos sectores y niveles de gobierno. Por lo tanto, la modernización de la gestión pública es una política de Estado que alcanza a todas las entidades públicas que lo conforman, sin afectar los niveles de autonomía que les confiere la ley. Compromete al Poder Ejecutivo, organismos autónomos, gobiernos descentralizados, instituciones políticas y la sociedad civil, a través de sus distintas organizaciones.”

5. Que, el numeral 3 de la Directiva N°013-2022-CG/NORM “Servicio de Control Simultaneo”, aprobada con Resolución de Contraloría N°218-2022CG de fecha 30 de mayo del 2020, indica que:

- **3 ALCANCE**

Las disposiciones contenidas en la presente Directiva son de obligatorio cumplimiento para:

(...)

Las entidades sujetas al Sistema Nacional de Control, de acuerdo a lo establecido en el artículo 3 de la Ley N° 27785, Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República, y sus modificatorias.”¹

6. Que, el subnumeral 6.1.1 del numeral 6.1 del punto 6 de la precitada Directiva indica que:

- 6. Disposiciones Generales
 - 6.1 Servicio de Control Simultaneo

El Servicio de Control Simultáneo forma parte de control gubernamental, el cual consiste en examinar de forma objetiva y sistemática los hitos de control o las actividades de un proceso en curso, con el objeto de identificar y comunicar oportunamente a la entidad o dependencia de la existencia de hechos que afecten o pueden afectar la continuidad, el resultado o el logro de los objetivos del proceso, a fin de que esta adopte las acciones preventivas y correctivas que correspondan, contribuyendo de esta forma a que el uso y destino de los recursos y bienes del Estado se realice con eficiencia, eficacia, transparencia, economía y legalidad. (...)

6.1.1 Características del Servicio de Control Simultaneo

¹Que, el artículo 3° de la Ley N° 27785, Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República, y sus modificatorias, indica en su literal b), que su aplicación recae sobre los “Gobiernos Regionales y **Locales** e instituciones y empresas pertenecientes a los mismos, por los recursos y bienes materia de su participación accionaria”





El Servicio de Control Simultáneo se caracteriza por ser:

- a) Oportuno
- b) Célere
- c) Sincrónico
- d) Preventivo

7. Así mismo, el literal b) del punto III, del numeral 6.1.8.2 de la Sexta Disposición de la precitada Directiva, indica que:

- **“6. Disposiciones Generales**
 - **6.1 Servicio de Control Simultaneo**

6.1.8 Seguimiento y Evaluación de Acciones respecto a las situaciones adversas comunicadas a la entidad o dependencia.

6.1.8.2 Situaciones adversas de los Informes emitidos como resultado del desarrollo del Servicio de Control Simultáneo

iii. En un plazo máximo de tres (3) días hábiles siguientes a las comunicaciones remitidas por la entidad o dependencia o la información que se obtenga a través de medios oficiales, respecto a las acciones correctivas o preventivas adoptadas en relación con las situaciones adversas, el Jefe de Comisión o el OCI, según corresponda, evalúa la información recibida, y registra el estado que corresponda a la situación adversa en el aplicativo informático de la Contraloría (...)

8. Que, en el artículo 1° de la Resolución Ministerial N°004-2016-PCM, se resuelve declarar la aprobación de:

- **“Artículo 1. – De la Aprobación**

Apruébese el uso obligatorio de la normal Técnica Peruana “ISO NTP/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2ª. Edición, en todas las entidades integrantes del Sistema Nacional de Información”

9. Es preciso señalar que, para el Ingeniero Dejan Kosutic, el ISO/IEC 27001 “es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2”, así mismo indica que, “puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o **pública**, pequeña o grande”²

² Kosutic Dejan , Advisera, ¿Qué es Norma ISO27001?, recuperado el 14 de diciembre del 2022.





MUNICIPALIDAD DE VILLA EL SALVADOR
OFICINA DE ASESORIA JURIDICA

10. Que, el artículo 2°, 3° y 4° de la Ley N°27658, Ley Marco de Modernización de la Gestión del Estado, establece que:

- **“Artículo 2.- Objeto de la ley**

La presente Ley tiene por objeto establecer los principios y la base legal para iniciar el proceso de modernización de la gestión del Estado, en todas sus instituciones e instancias.”

- **“Artículo 3.- Alcance de la ley**

La presente Ley es de aplicación en todas las dependencias de la Administración Pública a nivel nacional.”

- **“Artículo 4.- Finalidad del proceso de modernización de la gestión del Estado**

El proceso de modernización de la gestión del Estado tiene como finalidad fundamental la obtención de mayores niveles de eficiencia del aparato estatal, de manera que se logre una mejor atención a la ciudadanía, priorizando y optimizando el uso de los recursos públicos (...).”

11. Que, el numeral 5 y 6 del artículo 7° de la Ley N°27815, Ley del Código de Ética de la Función Pública, precisa lo siguiente:

- **“Artículo 7.- Deberes de la Función Pública**

El servidor público tiene los siguientes deberes:

(...)

- **5. Uso Adecuado de los Bienes del Estado**

Debe proteger y conservar los bienes del Estado, debiendo utilizar los que le fueran asignados para el desempeño de sus funciones de manera racional, evitando su abuso, derroche o desaprovechamiento, sin emplear o permitir que otros empleen los bienes del Estado para fines particulares o propósitos que no sean aquellos para los cuales hubieran sido específicamente destinados.

- **6. Responsabilidad**

Todo servidor público debe desarrollar sus funciones a cabalidad y en forma integral, asumiendo con pleno respeto su función pública. (...).”

12. Que, el artículo 3° de la Ley N°29733, Ley de Protección de Datos Personales, establece lo siguiente:

- **“Artículo 3. Ámbito de aplicación**





MUNICIPALIDAD DE VILLA EL SALVADOR
OFICINA DE ASESORIA JURIDICA

La presente Ley es de aplicación a los datos personales contenidos o destinados a ser contenidos en bancos de datos personales de administración pública y de administración privada, cuyo tratamiento se realiza en el territorio nacional. Son objeto de especial protección los datos sensibles. (...)

13. Que, el artículo 1° del Decreto Legislativo N°1412, Decreto Legislativo que Aprueba la Ley de Gobierno Digital, establece que:

- **“Artículo 1.- Objeto**

La presente Ley tiene por objeto establecer el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno.”

14. Así mismo, los numerales 6.1 y 6.2 del artículo 6° y el numeral 7.1 del artículo 7° del precitado Decreto Legislativo, señala en referencia al Gobierno Digital, que:

- **“Artículo 6.- Gobierno Digital**

6.1. El gobierno digital es el uso estratégico de las tecnologías digitales y datos en la Administración Pública para la creación de valor público. Se sustenta en un ecosistema compuesto por actores del sector público, ciudadanos y otros interesados, quienes apoyan en la implementación de iniciativas y acciones de diseño, creación de servicios digitales y contenidos, asegurando el pleno respeto de los derechos de los ciudadanos y personas en general en el entorno digital.

6.2. Comprende el conjunto de principios, políticas, normas, procedimientos, técnicas e instrumentos utilizados por las entidades de la Administración Pública en la gobernanza, gestión e implementación de tecnologías digitales para la digitalización de procesos, datos, contenidos y servicios digitales de valor para los ciudadanos.”

- **“Artículo 7.- Objetivos del Gobierno Digital**

Los objetivos del gobierno digital son:

7.1 Normar las actividades de gobernanza, gestión e implementación en materia de tecnologías digitales, identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos. (...)

15. Así mismo, el artículo 30° del Decreto Legislativo N°1412, Decreto Legislativo que Aprueba la Ley de Gobierno Digital, establece que:





- **“Artículo 30°.- De la Seguridad Digital**

La seguridad digital es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas.”

16. Con Resolución N°439-2021-GM-MVES se aprueba conformar el Comité de Gobierno Digital de la Municipalidad de Villa El Salvador, por el cual se resuelve en su artículo Primero que:

- **Artículo Primero.** - CONFORMAR el Comité de Gobierno Digital de la Municipalidad Distrital de Villa El Salvador, el mismo que estará integrado por los siguientes miembros:
 - **En representación del Titular de la Entidad, El Gerente Municipal.**
 - **El Gerente Municipal, Como Líder de Gobierno Digital.**

(...)”

17. Que, el numeral 14.2 y 14.3 del artículo 14° de la Ordenanza N° 441-MVES, Ordenanza que modifica la Estructura Orgánica de la Municipalidad Distrital de Villa El Salvador y el Reglamento de Organización y Funciones (ROF), con enfoque de Gestión de Resultados de la Municipalidad Distrital de Villa el Salvador aprobado con Ordenanza N° 369-MVES, respecto a su función normativa y reguladora, señala que:

- “14.2 Aprobar las disposiciones necesarias para la implementación del Sistema de Control Interno.”
- “14.3 Aprobar los procesos, procedimientos, directivas, reglamentos y demás normativas internas de carácter administrativo propuestas por las oficinas o gerencias de la Municipalidad; cuando corresponda y de acuerdo a la normatividad vigente.”

18. Que, el numeral 36.1 y 36.4 del artículo 36° de la Ordenanza N° 441-MVES, Ordenanza que modifica la Estructura Orgánica de la Municipalidad Distrital de Villa El Salvador y el Reglamento de Organización y Funciones (ROF), con enfoque de Gestión de Resultados de la Municipalidad Distrital de Villa el Salvador aprobado con Ordenanza N° 369-MVES, indica respecto a la función de planeamiento y función normativa y reguladora, que:

- “36.1 Diseñar el Plan de Contingencias Informático, el Plan de Seguridad de la Información, y otros planes que sean de su competencia.”

(...)





MUNICIPALIDAD DE VILLA EL SALVADOR
OFICINA DE ASESORIA JURIDICA

- “36.4 Proponer proyectos de normas Municipales en materia de su competencia, para la mejora de la gestión.”
19. Con Resolución de Alcaldía N°164-2021-ALC/MVES, se designa al Gerente Municipal en el Cargo de Líder de Gobierno Digital de la Municipalidad Distrital de Villa El Salvador, quien estará a cargo *“de coordinar objetivos, acciones y medidas para la transformación digital y despliegue del Gobierno Digital a nivel institucional, conforme a las políticas y directrices emitidos por la Presidencia del Consejo de Ministros, (...)”*
 20. Por lo antes expuesto, se colige que, la Subgerencia de la Unidad de Desarrollo Tecnológico ha propuesto el plan de *“Política de Seguridad de la Información de la Municipalidad Distrital de Villa El Salvador”* ello conforme a sus atribuciones preestablecidas en el ROF; así mismo, el Gerente Municipal de esta Corporación Edil será el encargado de aprobar la Política propuesta por la Subgerencia de la Unidad de desarrollo Tecnológico, debido a que es el representante de la Entidad y el Líder del Gobierno Digital, atribuciones conferidas mediante Resolución de Alcaldía N°164-2021-ALC/MVES, por el cual se designa al Gerente Municipal en el Cargo de Líder de Gobierno Digital de la Municipalidad Distrital de Villa El Salvador, así como con Resolución N°439-2021-GM-MVES que aprueba conformar el Comité de Gobierno Digital de la Municipalidad de Villa El Salvador, y a su función normativa y reguladora contemplada en el numeral 14.2 y 14.3 de la Ordenanza N° 441-MVES.
 21. Que, con Memorando Múltiple N°062-2021-OGA/MVES de fecha 17 de noviembre del 2021, la Oficina General de Administración, solicita a la Subgerencia de la Unidad de Desarrollo Tecnológico, que se remita el Plan de Acción de la Situación Adversa N°05 correspondiente a la *“Comunicación del informe de Orientación de Oficio N°20110-2021-CG/GRLIM-SOO-Implementación, Funcionalidad y Política de Seguridad del Sistema de Recaudación y Sistema de Administración Financiera de la Municipalidad de Villa El Salvador”*, el cual señala que esta Corporación Edil no cuenta con Políticas de Seguridad de la Información.
 22. Que, con Memorando Múltiple N°062-2021-OGA/MVES de fecha 17 de noviembre del 2021, la Oficina General de Administración, solicita a la Subgerencia de la Unidad de Desarrollo Tecnológico, que se remita el Plan de Acción de la Situación Adversa N°05 correspondiente a la *“Comunicación del informe de Orientación de Oficio N°20110-2021-CG/GRLIM-SOO-Implementación, Funcionalidad y Política de Seguridad del Sistema de Recaudación y Sistema de Administración Financiera de la Municipalidad de Villa El Salvador”*, el cual señala que esta Corporación Edil no cuenta con Políticas de Seguridad de la Información.
 23. Que, con Memorando N°925-2022-GM/MVES de fecha 13 de setiembre del 2022, la Oficina de la Gerencia Municipal remite a la Subgerencia de la Unidad de Desarrollo Tecnológico, el *“Reporte de Seguimiento de las acciones para el tratamiento de situaciones adversas resultantes de servicio de control simultaneo” del 01 al 31 de agosto del 2022*, en solicitud de cumplir con la ejecución de los Planes de Acción de las Situaciones Adversas remitidas por el Órgano de Control Interno -OCI.





**MUNICIPALIDAD DE VILLA EL SALVADOR
OFICINA DE ASESORIA JURIDICA**

24. Informe N°0169-2022-UDT-OGA/MVES de fecha 25 de noviembre del 2022, la Subgerencia de la Unidad de Desarrollo Tecnológico remite a la Oficina de la Gerencia Municipal el Proyecto de Política de Seguridad de la Información de la Municipalidad Distrital de Villa El Salvador, para que la Gerencia de la Oficina de Asesoría Jurídica determine el instrumento legal a Utilizarse para su aprobación.
25. Que, teniendo a la vista los actuados y en concordancia con los fundamentos facticos y jurídicos del presente informe, y tomando en consideración lo exhortado por el Informe de Orientación N°20410-2021-CG/GRLIM-SOO en relación a la Situación Adversa N°05, este despacho de la Gerencia de la Oficina de Asesoría Jurídica es de la opinión que, es **LEGALMENTE VIABLE** la aprobación del Plan de Política de Seguridad de la Información, con el fin de atender la Situación Adversa N°05 correspondiente al Informe de Orientación N°20410-2021-CG/GRLIM-SOO. Así mismo, la aprobación de dicho Plan, se perfeccionará mediante Resolución de Gerencia Municipal, ello en conformidad con lo resuelto en el artículo 1° y 2° de la Resolución N°439-2021-GM-MVES y del numeral 14.2 y 14.3 del artículo 14° de la Ordenanza N° 441-MVES.

IV. OPINIÓN:

En virtud de lo expuesto en el análisis del presente informe, esta Oficina de Asesoría Jurídica, es de la **OPINION** que:

1. Que **ES LEGALMENTE VIABLE** la aprobación del Plan de Política de Seguridad de la Información, con el fin de atender la Situación Adversa N°05 correspondiente al Informe de Orientación N°20410-2021-CG/GRLIM-SOO. Así mismo, la aprobación de dicho Plan, **se perfeccionará mediante Resolución de Gerencia Municipal**, ello en conformidad al artículo 194° de la Constitución Política del Perú, así como al artículo II del Título Preliminar de la Ley N° 27972, al artículo 1° y el artículo 2° del Decreto Supremo N°004-2013-PCM, al numeral 3, subnumeral 6.1 del numeral 6 de la Directiva N°013-2022-CG/NORM "Servicio de Control Simultaneo", aprobada con Resolución de Contraloría N°218-2022CG, como al artículo 1° de la Resolución Ministerial N°004-2016-PCM, y a los numerales 6.1 y 6.2 del artículo 6° y el numeral 7.1 del artículo 7° Decreto Legislativo N°1412, Decreto Legislativo que Aprueba la Ley de Gobierno Digital, a su vez, al artículo 1° de la Resolución de Alcaldía N°164-2021-ALC/MVES, así como del artículo 1° y 2° de la Resolución N°439-2021-GM-MVES que aprueba conformar el Comité de Gobierno Digital de la Municipalidad de Villa El Salvador y del numeral 14.2 y 14.3 del artículo 14° de la Ordenanza N° 441-MVES, Ordenanza que modifica la Estructura Orgánica de la Municipalidad Distrital de Villa El Salvador y el Reglamento de Organización y Funciones (ROF), con enfoque de Gestión de Resultados de la Municipalidad Distrital de Villa el Salvador aprobado con Ordenanza N° 369-MVES.





**MUNICIPALIDAD DE VILLA EL SALVADOR
OFICINA DE ASESORIA JURIDICA**

Se remiten a vuestro despacho los antecedentes administrativos a fin de que se continúe con el trámite que corresponda.

Atentamente,



MUNICIPALIDAD DE VILLA EL SALVADOR
Abg. Shirlet M. Castro Gonzales
Gerente de Asesoría Jurídica

1



TEL'S 287-1394 - 287-8999
TELEFAX 287-1071
www.munives.gob.pe

MEMORÁNDUM N° 1219 - 2022-GM/MVES

A : **Abog. Shirlet Marley Castro Gonzales**
Gerente de Asesoría Jurídica

De : **Abog. José Luis Espichan Pérez**
Gerente Municipal



ASUNTO : Sobre Revisión y Aprobación de Política de Seguridad de la Información de la Municipalidad Distrital de Villa El Salvador.

REF : a) Informe N° 169-2022-UDT-OGA/MVES

FECHA : Villa el Salvador, 29 de Noviembre del 2022

Me dirijo a usted en atención al documento de la referencia a) mediante el cual al Subgerente de la Unidad de Desarrollo Tecnológico, remite para su evaluación por parte del despacho de Asesoría Jurídica el proyecto de **"Políticas de Seguridad de la Información"**, en merito a la Situación Adversa N° 5 del Informe de Orientación de Oficio N° 20410-2021-CG/GRILIM-SOO - "Implementación, Funcionalidad y Políticas de Seguridad del Sistema de Recaudación y Sistema de Administración Financiera de la Municipalidad de Villa El Salvador", a fin de que se determine el instrumento legal a utilizarse para su aprobación y continuación del procedimiento según su estado.

En relación a ello, se remite los actuados a su despacho, a fin de que conforme a su función establecida en el Numeral 24.9, del Artículo 24°, de la Ordenanza N° 441-MVES, emita Opinión Legal correspondiente en el plazo de Cinco (05) Días Hábiles.

Atentamente.

MUNICIPALIDAD DE VILLA EL SALVADOR
GERENCIA MUNICIPAL

JOSE LUIS ESPICHAN PÉREZ
GERENTE

INFORME N° 0169-2022-UDT-OGA/MVES

A : **JOSE LUIS ESPICHAN PEREZ**
Gerente Municipal

DE : **ING. JOSE MANUEL GUIZADO CASTILLO**
Sub Gerente de la Unidad de Desarrollo Tecnológico

ASUNTO : **Revisión y Aprobación de Política de Seguridad de la Información de la Municipalidad Distrital de Villa el Salvador**

REF. : a). Memorando Múltiple N°925-2022-GM//MVES

FECHA : Villa El Salvador, 25 de noviembre del 2022



Mediante documento de referencia a) de fecha 13SET22 la Gerencia Municipal remitió a esta Unidad, el "Reporte de Seguimiento de las acciones para el tratamiento de situaciones adversas resultantes de servicio de control simultaneo" del 01 al 31 de agosto del 2022", en solicitud de cumplir con la ejecución de los Planes de Acción de las Situaciones Adversas remitidas por OCI.

Que, la situación adversa Nro.05 del Informe de Orientación de Oficio N° 20410-2021-CG/GRLIM-SOO señala que; "la Entidad no cuenta con políticas de seguridad de la información aprobadas, careciendo de controles definidos para identificar las deficiencias en el diseño e implementación de los sistemas y el tratamiento de los riesgos y amenazas, afectando la protección de los activos de información".

I. ANTECEDENTES:

- Mediante el Memorando Múltiple N.° 038-2022-OG/MVES de fecha 11 de agosto del 2022, la Oficina General de Administración, solicita el "Reporte de Seguimiento de las acciones para el tratamiento de situaciones adversas resultantes de servicio de control simultaneo" a Julio 2022, señalando entre otros, situaciones adversas referente a la seguridad de los activos de la información perteneciente a la Municipalidad Distrital Villa El Salvador.
- Mediante el Informe 0213-2021 UDT-OGA/MVES de fecha 23 de noviembre del 2021, esta unidad, remite a la Oficina General de Administración el Plan de Acción para implementar la Situación Adversa Nro. 05 correspondiente al Informe de Orientación de Oficio N.° 20410-2021-CG/GRLIM-SOO, en respuesta a la situación adversa Nro.05 entre otros contenidas en el informe en la que señala que; "La Entidad no cuenta con políticas de seguridad de la información aprobadas, careciendo de controles definidos para identificar las deficiencias en el diseño e implementación de los sistemas y el tratamiento de los riesgos y amenazas, afectando la protección de los activos de información."
- Mediante el Memorando múltiple N.° 062-2021-OGA/MVES de fecha 17 de noviembre del 2021, la Oficina General de Administración, solicita a esta Unidad se remite el Plan de Acción de la Situación Adversa N°5 correspondiente a la "Comunicación del informe de Orientación de Oficio N.° 20110-2021-CG/GRLIM-SOO - "Implementación, Funcionalidad y Política de Seguridad del Sistema de Recaudación y Sistema de Administración Financiera de la Municipalidad de Villa El Salvador", que señala, la Entidad no cuenta con políticas de seguridad de la información.





II. BASE LEGAL:

- Decreto Supremo N°. 004-2013-PCM, publicada el 09 de enero del 2013, que aprueba la Política Nacional de Modernización de la Gestión Pública.
- Resolución de Jefatura N° 090-95-INEI, aprueba la Directiva N° 008-95-INEI/SJI, "Recomendaciones Técnicas para la Protección Física de los Equipos y Medios de Procesamiento de la Información en la Administración Pública".
- Resolución Ministerial N° 246-2007-PCM, de fecha 22 de agosto 2007, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnológica de la Información. Código de buenas prácticas para la Gestión de la Seguridad de la Información.
- Resolución Ministerial N° 197-2011-PCM, que establece fecha límite para que diversas entidades de la Administración Pública implementen el plan de seguridad de la información dispuesto en la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información".
- Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "ISO NTP/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución de Contraloría N° 320-2006-CG, "Normas de Control Interno para las Entidades del Estado"

III. ANALISIS:

- Con Informe 0213-2021 UDT-OGA/MVES, la Unidad de Desarrollo Tecnológico remite a la Oficina General de Administración el Plan de Acción de la Situación Adversa Nro. 05 Informe de Orientación de Oficio N.º 20410-2021-CG/GRILIM-SOO - "Implementación, Funcionalidad y Políticas de Seguridad del Sistema de Recaudación y Sistema de Administración Financiera de la Municipalidad de Villa El Salvador, señalando un plazo establecido y acciones a concretar para la elaboración de las Políticas de Seguridad de la Información.
- Con Memorando múltiple N.º 044-2022-OGA/MVES, la Oficina General de Administración remite a la Unidad de Desarrollo Tecnológico el Reporte de "Seguimiento de la acción para el tratamiento de situaciones adversas resultantes de servicio de Control Simultaneo", solicitando cumplir con la ejecución de los Planes de Acción de las Situaciones Adversas N°5 entre otros remitidas a OCI.
- Con el Informe N°0145-2022-UDT-OGA/MVES, la Unidad de Desarrollo Tecnológico remite el Plan de Gestión de la Seguridad de la Información a la Gerencia Municipal, indicando una de las actividades: "Establecer una Política de Seguridad de la Información".





- ISO/IEC 27001 es un estándar para la seguridad de la información (Information Technology - Security Techniques - Information Security Management Systems - Requirements) aprobado y publicado como estándar internacional en octubre de 2005 por la International Organization for Standardization y por la International Electrotechnical Commission, especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información según el conocido "Ciclo de Deming": denotado por las siglas PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar).
- Cabe precisar que, los puntos 1) y 4) del artículo 36 de Reglamento de Organización y Funciones (ROF) de la Municipalidad Distrital de Villa El Salvador, señala "Diseñar el Plan de Contingencia Informático, el Plan de Seguridad de la Información, y otros planes que sean de su competencia", y, "Proponer proyectos de normas municipales en materia de su competencia para la mejora de la gestión", como las funciones de Planeamiento y Normativa de la unidad, respectivamente.

En consecuencia, en cumplimiento a lo solicitado por el Órgano de Control Institucional, se traslada las Políticas de Seguridad de la Información para su derivación a la Oficina del despacho de Asesoría Jurídica a fin de que determine el instrumento legal a utilizarse para su aprobación, correspondiente a la Situación Adversa N°5 del Informe de Orientación de Oficio N.º 20410-2021-CG/GRILIM-SOO - "*Implementación, Funcionalidad y Políticas de Seguridad del Sistema de Recaudación y Sistema de Administración Financiera de la Municipalidad de Villa El Salvador*" y en cumplimiento de una de las actividades establecidas en el Plan de Gestión de Seguridad de la Información, en ochenta y uno (81) folios.

Por lo expuesto, sirvase continuar con el procedimiento según su estado a fin de que sea aprobado por acta resolutive determinado por el despacho de Asesoría Jurídica.

Atentamente,



MUNICIPALIDAD DE VILLA EL SALVADOR
UNIDAD DE DESARROLLO TECNOLÓGICO

Ing. Juan Manuel Guizado Castillo
SUB - GERENTE

MEMORANDO N° 925 -2022-GM/MVES



: Ing. José Manuel Guizado Castillo
SubGerente de la Unidad de Desarrollo Tecnológico

DE : Abg. José Luis Espichán Pérez
Gerente Municipal

ASUNTO : Servicio Relacionado "Seguimiento de las acciones para el tratamiento de Situaciones adversas resultantes del servicio de control simultáneo" del 1 al 31 de agosto de 2022

REFERENCIA : a) Proveído N° 0086-2022-ALC/MVES de fecha 12.09.2022
b) Oficio N° 000080-2022-CG/OC2696 de fecha 09.09.2022
c) (Cedula de notificación electrónica N° 00000014-2022-CG/2696

FECHA : Villa El Salvador, 13 de setiembre de 2022

Tengo el agrado de dirigirme a usted, en relación al documento de la referencia a) recepcionado con fecha 12.09.2022; por el cual el despacho de Alcaldía traslada el documento de la referencia b); en que el Órgano de Control Institucional OCI remite el reporte del "**Seguimiento a las acciones para el tratamiento de situaciones adversas resultantes del servicio de control simultáneo periodo: del 1 al 31 de agosto de 2022**" en el cual se advierte que a la fecha existen situaciones adversas con demoras en la implementación de acciones correctivas y/o preventivas; y que se disponga la respectiva implementación dentro los plazos establecidos; del área de su competencia de corresponder; por lo que; se le **EXHORTA** de atención inmediata a los requerimientos solicitados por el OCI; conforme lo establece la Directiva N° 013-2022-CG/NORM "Servicio de Control Simultáneo " aprobada con resolución de Contraioría N° 218-2022-CG de 30 de mayo de 2022.

En tal sentido, proceda a remitir lo solicitado al OCI; dentro del plazo de **cinco (5) días**; dando cuenta a este despacho; bajo responsabilidad funcional y administrativa. bajo expreso apercibimiento de remitir los actuados a la Secretaría Técnica de procesos disciplinarios para las acciones correspondientes (Se adjunta documentos de la referencia y reporte del OCI).

Atentamente,



MUNICIPALIDAD DE VILLA EL SALVADOR
GERENCIA MUNICIPAL

JOSE LUIS ESPICHAN PEREZ
GERENTE



POLITICA DE SEGURIDAD DE LA INFORMACION



ROL	CARGO	NOMBRE
Elaborado por:	Subgerente de Unidad de Desarrollo Tecnológico	Ing. José Manuel Guizado Castillo
Revisada por:		
Aprobada por:		





MUNICIPALIDAD DE VILLA EL SALVADOR

Año: 2022

POLITICAS DE SEGURIDAD DE LA INFORMACION

Versión: 1.0

Página: 2 de 72

CONTROL DE CAMBIOS

N° Versión	Fecha	Descripción de cambio	Responsable del Documento



	MUNICIPALIDAD DE VILLA EL SALVADOR	Año: 2022
	POLITICAS DE SEGURIDAD DE LA INFORMACION	Versión: 1.0
		Página: 3 de 72

1. OBJETIVO

Establecer procedimientos de seguridad de la información para proteger los recursos de la información de la Municipalidad Distrital de Villa El Salvador, y las Tecnologías utilizadas para su procesamiento, mediante controles que permitan mitigar los riesgos de seguridad de la información, en el marco de la NTP ISO/IEC 27001:2014.

1.1. Objetivo Específicos

- 1.1.1. Conservar, salvaguardar y proteger la información producida por los procesos que se realizan en la institución presentada al ciudadano a través de los diferentes medios, así como disminuir los riesgos en la gestión de la información por parte del usuario dentro de la red Municipal.
- 1.1.2. Establecer las reglas a seguir y las responsabilidades de los usuarios sobre el uso de información.

2. ALCANCES

El presente documento tiene alcance a todos los servidores, funcionarios, proveedores de servicio bajo contrato y locadores que presten servicio en general, que tengan acceso a los activos de la información de la Municipalidad Distrital de Villa El Salvador.

3. BASE LEGAL

- 3.1. Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.
- 3.2. Ley N° 27815, Ley del Código de Ética de la Función Pública.
- 3.3. Ley N° 29733, Ley de Protección de Datos Personales.
- 3.4. Ley N° 27927, Ley que modifica la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública, del 04 febrero de 2003
- 3.5. Resolución N° 129-2014/CNB-INDECOPI, que aprueba la Norma Técnica Peruana "NTPISO/IEC 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos. 2ª Edición".
- 3.6. Resolución Ministerial N° 004-2016-PCM, que aprueba el uso Obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistema de Gestión de Seguridad de la Información. Requisitos 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
- 3.7. Resolución Ministerial N° 119-2018-PCM, que dispone de la creación de un Comité de Gobierno Digital en cada entidad de la administración Pública.
- 3.8. Resolución de Alcaldía N° 164-2021-ALC/MVES, asigna al Gerente Municipal en el cargo de Líder de Gobierno Digital de la Municipalidad Distrital de Villa El Salvador.
- 3.9. Resolución N° 439-2021-GM-MVES, que aprueba conformar el Comité de Gobierno Digital de la Municipalidad de Villa El Salvador.

4. GLOSARIO DE TERMINOS

- 4.1. **Activo de Información:** Información que tiene valor para la Entidad. Se considera también los recursos humanos, tecnológicos que intervienen en el tratamiento directo o indirecto de la información, así como sus procesos y actividades.
- 4.2. **Amenaza:** Incidente no deseado que puede causar daños a un sistema u organización.
- 4.3. **Confidencialidad:** Propiedad de la información que hace que no esté disponible o que sea revelada a individuos o entidades no autorizados.
- 4.4. **Control:** Conducto para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la entidad que pueden ser de naturaleza administrativa, técnica, de gestión o legal.



- 4.5. **Disponibilidad:** Propiedad de ser accesible y utilizable ante la demanda de una entidad autorizada.
- 4.6. **Gestión de riesgo:** Políticas de gestión procedimientos y practicas a las actividades de comunicación, consulta, establecimiento del contexto e identificación, análisis, evaluación, tratamiento, seguimiento y revisión de riesgos.
- 4.7. **Incidente de Seguridad de la Información:** Evento no deseado que genera amenaza a la seguridad de la información y que tiene una probabilidad significativa de comprometer a la operativa en la Entidad.
- 4.8. **Información:** Cualquier forma de registro de contenidos susceptibles a ser procesados, distribuidos y almacenados, pudiendo estar en formato electrónico, óptico, magnéticos u otro medio de almacenamiento.
- 4.9. **Integridad:** Propiedad de salvaguardar la exactitud e integridad de la información y activos asociados.
- 4.10. **Locador:** Personal contratado como tercero para desarrollar determinado servicio a favor de la Entidad.
- 4.11. **Sistema de Gestión de la Seguridad de la Información (SGSI):** Es un componente del sistema de gestión de una organización, con base en un enfoque de riesgos, que tiene como función establecer, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. El SGSI está conformado por políticas, procedimientos, directrices, recursos y actividades asociadas, gestionadas por la organización, en la búsqueda de la protección de sus activos de información.
- 4.12. **Oficial de Seguridad de la Información:** El Oficial de Seguridad de la Información o quien haga de sus veces depende de la Unidad de Desarrollo Tecnológico, es el responsable del Sistema de Gestión de la Seguridad de la Información (SGSI) y reporta al Comité de Gobierno Digital (CGD).
- 4.13. **Plan de Contingencia:** Estrategia proactiva que te ayudara a abordar las situaciones negativas y garantizar la continuidad del negocio.
- 4.14. **Propietario del Activo de Información:** Es el funcionario asignado de garantizar que el activo asignado bajo su responsabilidad esté protegido con los controles definidos en el SGSI y que le apliquen a dicho activo; es el responsable por la afectación de la confidencialidad, integridad y disponibilidad del mismo, en cualquiera de los procesos que se encuentre involucrado.
- 4.15. **Proveedor:** Empresa que brinda servicios a la Municipalidad, en el caso que, el proveedor requiera los accesos a los activos de la información y/o a los servicios TI de la entidad, se le otorgará los permisos necesarios hasta culminar sus servicios y será monitoreado por la unidad orgánica al cual fue contratado.
- 4.16. **Riesgo:** Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de aquello que se espera, sea positivo, negativo o ambos. Los objetivos pueden tener aspectos diferentes (económicos, de imagen institucional, etc.) y se pueden aplicar a niveles diferentes (operativo, estratégico, organización).
- 4.17. **Seguridad de la Información:** Consiste en acciones orientadas a preservar la integridad, confidencialidad y disponibilidad de la información y los activos asociados a su tratamiento independiente de la forma en la que la información se encuentre.
- 4.18. **Sensibilización:** Es un proceso que tiene como objetivo principal impactar sobre el comportamiento de una población o reforzar buenas prácticas sobre algún tema en particular.
- 4.19. **Servidor:** Personal que desempeña un empleo, cargo o comisión subordinada al Estado.
- 4.20. **UA:** Unidad de Abastecimiento, es un órgano de apoyo, encargado de planificar, normar, promocionar, ejecutar y controlar el funcionamiento del Sistema Nacional de Abastecimiento.
- 4.21. **UDT:** Unidad de Desarrollo Tecnológico, es un órgano de apoyo, encargado de gestionar los recursos TI de la Municipalidad Distrital de Villa El Salvador
- 4.22. **UGRH:** Unidad de Gestión de Recursos Humanos, órgano de apoyo, encargado de planificar, normar, promocionar, ejecutar y controlar el funcionamiento del Sistema Nacional de Gestión de Recursos Humanos.
- 4.23. **Vulnerabilidad:** Debilidad identificada sobre un activo y que puede ser aprovechado por una amenaza para causar una afectación sobre la confidencialidad, integridad o disponibilidad de dicho activo.



	MUNICIPALIDAD DE VILLA EL SALVADOR	Año: 2022
	POLITICAS DE SEGURIDAD DE LA INFORMACION	Versión: 1.0
		Página: 5 de 72

5. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La Municipalidad Distrital de Villa El Salvador reconoce la información como un activo vital para la Institución comprometiéndose a mantener su integridad, confidencialidad y disponibilidad, mediante la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), bajo el cual gestiona los riesgos de sus activos de la información, así mismos del marco legal establecido promueve la mejora continua del Sistema de Gestión de Seguridad de la Información.

6. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

- 6.1. Alinear la seguridad de información con la estrategia de negocio para apoyar los objetivos de la organización.
- 6.2. Análisis de gestión de riesgos
- 6.3. Optimizar las inversiones en seguridad en apoyo a los objetivos de negocio
- 6.4. Utilización del conocimiento y la infraestructura de seguridad con eficiencia y efectividad.
- 6.5. Monitorización y reporte de los procesos para garantizar que se alcanzan los objetivos.
- 6.6. Emplear un enfoque de sistema para planificar, implementar, monitorear y gestionar la seguridad de la información

7. POLÍTICAS ESPECIFICAS

7.1. Política de Seguridad de la Información

- 7.1.1. La Municipalidad Distrital de Villa El Salvador con el soporte del Oficial de Seguridad de la Información o quien haga a sus veces, debe elaborar documentos normativos de Seguridad de la Información a fin de proteger la información de la Entidad.
- 7.1.2. La Municipalidad Distrital de Villa El Salvador con el soporte del Oficial de Seguridad de la Información o quien haga a sus veces, debe difundir periódicamente las Políticas Especificas de Seguridad de la Información de la Entidad.
- 7.1.3. La Municipalidad Distrital de Villa El Salvador con el soporte del Oficial de Seguridad de la Información o quien haga a sus veces, debe monitorear el cumplimiento de la presente política, y actualizar las políticas Especificas en el periodo de un año; contando a partir de la aprobación y publicación del presente documento.

7.2. Política de Organización de Seguridad de la Información

7.2.1. Roles y Responsabilidades

- Oficial de Seguridad de la Información o quien haga a sus veces, debe proponer la estructura organizacional y los roles y responsabilidad para la gestión de la seguridad de información en la Entidad.
- El Comité de Gobierno Digital debe aprobar la estructura organizacional para la gestión de la seguridad de la información, también aprobar los roles y responsabilidades de los locadores que forman parte de la referida estructura.
- Las funciones y responsabilidades del personal serán detalladas en el documento Manual de Funciones y Responsabilidades del Sistema de Gestión de Seguridad de la Información.

7.2.2. Dispositivos Móviles

- El uso de dispositivos de computación móvil como equipos portátiles, teléfonos móviles, tabletas, entre otros, está permitido para el acceso a los aplicativos Web institucionales y el acceso al correo electrónico institucional, para lo cual el servidor público o locador





tendrá asignado un usuario y contraseña con los respectivos niveles de acceso de acuerdo con el rol asignado.

- Los dispositivos móviles de propiedad de la institución, asignados a los servidores públicos son para uso de las actividades propias del cargo o desempeño laboral y deben estar protegidos con una contraseña de inicio de sesión.
- Se debe asegurar que los servicios de TI ofrecidos, solo se accedan desde los equipos de cómputo y dispositivos móviles proporcionados por la Entidad, o desde aquellos debidamente autorizados.
- Está prohibido el uso de dispositivos móviles de propiedad de la Entidad para guardar información personal; igualmente está prohibido realizar instalación de software no autorizado.
- El servidor público de la institución debe proteger sus equipos móviles, no debiendo entregarlos a otra persona, en particular en aquellos dispositivos inteligentes que almacenan información sensible de la Entidad. En estos casos, incluso los mensajes recibidos de números o remitentes desconocidos deben ser denegados y borrados sin ser abiertos.
- El Municipalidad Distrital de Villa El Salvador a través de la UDT debe mantener una administración centralizada de las características de los dispositivos móviles.

7.2.3. Acceso Remoto o Trabajo en Casa.

- El Servidor y locador que solicita laborar bajo el termino acceso remoto, debe cumplir con la presente política y cualquier otra normativa interna relacionada a seguridad de la información, protección y confidencialidad de los datos.
- La UDT de la Municipalidad Distrital de Villa El Salvador debe definir los procedimientos para asignar y aprobar el acceso remoto al servidor y locador de la Entidad.
- El servidor y locador de la Entidad que requiera laborar bajo el termino acceso remoto, debe guardar confidencialidad de la información proporcionada por la institución para la prestación de servicios y no deberá almacenar información de la Institución en el equipo de cómputo desde donde se conecta remotamente.
- Todo servidor, locador y proveedor que solicite acceso remoto para acceder a los recursos y servicios internos de la Entidad, el cual será habilitado, autorizado y supervisado por UDT de la Municipalidad Distrital de Villa El Salvador, debe ser con previa autorización del Gerente, Subgerentes o jefe de área de la unidad orgánica a la que pertenece; mediante el documento y formulario correspondiente indicando tiempo y motivo del sustento de la solicitud. Además, el rango de horario permitido para el acceso remoto es de lunes a viernes de 08 horas hasta las 18 horas.
- El Gerente, Subgerente o jefe de área que autoriza la solicitud de acceso remoto, es responsable de evaluar la adecuada correspondencia con aquellos roles que realmente requieren el acceso por cumplimiento de sus funciones; de forma que se preserve la seguridad de la información de la institución a la que accederá el locador.
- Todo servidor y locador que cuente con acceso remoto debe proteger la información a la que tiene acceso cumpliendo lo siguiente:
 - La Conexión debe ser en ambientes físicos seguros.
 - Debe bloquear el equipo de computo desde el cual se conecta, cuando se traslade a otro lugar.
 - Cerrar sesión en el acceso remoto al finalizar sus actividades.





MUNICIPALIDAD DE VILLA EL SALVADOR	Año: 2022
POLITICAS DE SEGURIDAD DE LA INFORMACION	Versión: 1.0
	Página: 7 de 72

- Se encuentra prohibido cualquier otro mecanismo técnico de acceso remoto que permita el acceso desde redes externas a la red de la Municipalidad o viceversa.
- La asistencia remota interna es realizada sólo por el personal técnico de UDT de la Municipalidad Distrital de Villa El Salvador, para lo cual se utilizarán conexiones con protocolos seguros; no está autorizado el acceso remoto entre locadores de otras unidades orgánicas.

7.3. Políticas de Seguridad de Información vinculado a Recursos Humanos

7.3.1. Antes del Empleo

- La UGRH de la Municipalidad Distrital de Villa El Salvador debe verificar los antecedentes laborales de acuerdo a las leyes y regulaciones vigentes, y las competencias requeridas para el puesto laboral.
- La UGRH de la Municipalidad Distrital de Villa el Salvador, debe establecer en los acuerdos contractuales de empleo, cláusulas de confidencialidad, declaración de responsabilidades con respecto a la seguridad de la información, y clausulas respecto a las leyes de derecho de autor o protección de datos, según corresponda. Dichos acuerdos estarán vigentes hasta la finalización del contrato.

7.3.2. Durante el Empleo

- La UGRH de la Municipalidad Distrital de Villa El Salvador, debe informar a los servidores contratados, acerca de sus responsabilidades con respecto a la Seguridad de la Información establecidas en la política.
- La UGRH de la Municipalidad Distrital de Villa El Salvador, debe comunicar a la Unidad de Desarrollo Tecnológico, cuando corresponda, el inicio o rotación del vínculo laboral de los servidores para el otorgamiento de acceso a los Sistemas de Información.
- La Secretaria Técnica de la UGRH de la Municipalidad Distrital de Villa El Salvador puede iniciar procesos disciplinarios y/o acciones legales pertinentes a los servidores que incumplan las Políticas de Seguridad de la Información y Normativas de Seguridad de la Información, siempre y cuando sean solicitados por el jefe de la unidad orgánica al cual corresponde.
- Todo servidor y locador debe cumplir con lo dispuesto en las Políticas de Seguridad de la Información, así como con toda normativa relacionada con la seguridad de la información emitidas por la institución.
- La UGRH de la Municipalidad Distrital de Villa El Salvador con apoyo del Oficial de Seguridad de la Información o quien haga de sus veces, deben asegurar que los servidores reciban la sensibilización y capacitación en seguridad de la información.
- Todo producto, desarrollo, investigaciones, avances tecnológicos por los servidores y locadores serán de propiedad de la Municipalidad Distrital de Villa El Salvador.

7.3.3. Después del Empleo

- La UGRH debe informar a la UDT de la Municipalidad Distrital de Villa El Salvador, la finalización de las funciones laborales del servidor al día siguiente de tomado conocimiento de la culminación, con la finalidad de realizar la desactivación de los accesos a los Sistemas de Información y demás recursos.
- En caso que el servidor tenga accesos físicos, también deben ser removidas o bloqueadas (permisos de acceso a lugares físico, por ejemplo: llaves de puerta o armarios, acceso con lectores biométricos).





MUNICIPALIDAD DE VILLA EL SALVADOR	Año:	2022
	Versión:	1.0
	Página:	8 de 72

- Todo Servidor, al término de su relación contractual con la Municipalidad Distrital de Villa El Salvador, debe poner a disposición a su jefe inmediato, todos los documentos físicos o digitales que le fueron asignados o elaborados, como parte de sus funciones.

7.4. Política de Gestión de Seguridad de Activos de Información

7.4.1. Responsabilidad y Uso de Activos de Información

- La UDT de la Municipalidad Distrital de Villa El Salvador, debe gestionar y mantener un inventario de activos de información actualizado, procurando la vigencia tecnológica de tales recursos; así mismo, el inventario debe detallar el responsable del activo de la información.
- La UDT de la Municipalidad Distrital de Villa El Salvador, debe formular y establecer las reglas para el uso apropiado de los activos de la información, cumpliendo con el marco normativo y las políticas de seguridad de la información. Y asegurar su difusión y cumplimiento por todo el personal de la Entidad.
- Los servidores y locadores deben usar los activos de información solo y exclusivamente para fines laborales en cumplimiento con el marco normativo.
- Los servidores y locadores no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo (hardware y software), tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla institucional
- Los servidores y locadores deberán retomar todos los activos de la institución que le fueron otorgados para el desarrollo de sus funciones, al término de su contrato.
- La Adquisición de bienes y/o servicios, donde se incluyan equipos informáticos como parte integrante o complementaria de otros, serán validados por la UDT de la Municipalidad Distrital de Villa El Salvador.
- La UDT de la Municipalidad Distrital de Villa El Salvador, deberá validar que los equipos informáticos cumplan con las especificaciones indicadas en TDR de la Solicitud de compra.
- Todos los recursos de TI asignados por la Municipalidad a un usuario deben ser devueltos por este al término de sus funciones u obligaciones contractuales, o cuando la necesidad operativa que justifico la asignación ya no sea vigente.
- Toda Unidad Orgánica de la Municipalidad Distrital de Villa El Salvador, debe informar a los locadores y proveedores contratados, acerca de sus responsabilidades con respecto a la Seguridad de la Información establecidas en la política.

7.4.2. Clasificación de la Información

- Los propietarios de los activos de la información son los encargados de clasificar la información que manejan en cada proceso, de acuerdo a lo establecido en la Ley de Transparencia y Acceso a la Información Pública: reservada, confidencial y/o pública.
- Los propietarios de los activos de información deben etiquetar la información según la clasificación realizada y que sea conforme a los lineamientos establecidos por la Institución.

7.4.3. Control de medios removibles

- El traslado de medios removibles (disco externo, dispositivos móviles, DVD, CD, memorias USB, agendas electrónicas, etc.) fuera de las instalaciones de la



	MUNICIPALIDAD DE VILLA EL SALVADOR	Año: 2022
	POLITICAS DE SEGURIDAD DE LA INFORMACION	Versión: 1.0
		Página: 9 de 72

Municipalidad Distrital de Villa El Salvador, que contengan información confidencial, se encuentra prohibida, excepto con la autorización la alta gerencia.

- Los responsables de los órganos y unidades orgánicas deben autorizar al locador el uso del medio removible en caso lo amerite.
- Todo locador que requiera conectar medio removible a su equipo de cómputo, deberá asegurarse que este analizado por un el software antimalware/antivirus.

7.5. Políticas de Gestión de Acceso

7.5.1. Requisitos de la Institución en el Control de Acceso

- La UA de la Municipalidad Distrital de Villa El Salvador, encargado de la seguridad física en la Entidad, debe establecer directivas para el control de acceso físico a la entidad y sus ambientes.
- El acceso a los activos de información, servicios, instalaciones físicas y en general cualquier recurso de información de la Municipalidad Distrital de Villa El Salvador estará permitido únicamente a los usuarios autorizados, de acuerdo con los roles y permisos asignados.
- Los requerimientos y atenciones para acceso al sistema de información de la Municipalidad Distrital de Villa El Salvador deben ser solicitados en lo formatos establecidos en las directivas para este propósito, con la respectiva autorización de la unidad al que pertenece.
- El servidor y locador de la Municipalidad Distrital de Villa El Salvador debe tener acceso solamente a la red y a servicios de red que hayan sido específicamente autorizados a usar.

7.5.2. Gestión de Acceso de Usuario

- Los encargados de cada unidad orgánica de la entidad deben autorizar y luego solicitar a la UDT de la Municipalidad Distrital de Villa El Salvador, el acceso a los sistemas de información y servicios informáticos para el servidor y locador bajo su cargo.
- Los encargados de cada unidad orgánica de la entidad, están en la obligación de informar la culminación de servicio de servidores, locadores y proveedores para la baja de las cuentas de acceso, cuales fueron asignados durante su desempeño laboral, mediante los formatos establecidos por la UDT de la Municipalidad Distrital de Villa El Salvador.
- La UDT de la Municipalidad Distrital de Villa El Salvador, debe guardar los registros de autorización de acceso de los usuarios (activación o baja de cuenta) por parte de encargado de la unidad orgánica de la entidad.
- La UDT de la Municipalidad Distrital de Villa El Salvador, debe mantener actualizada las cuentas de usuario de acceso del sistema de información que gestionan, en coordinación con los encargados de cada unidad orgánica de la entidad.
- La nomenclatura para nombrar toda cuenta de usuario será la letra inicial del primer nombre seguido por el apellido paterno más la letra inicial del apellido materno. En caso de coincidir el nombre y apellidos con los de otro usuario, se deber considerar, además, la letra inicial del segundo nombre. De persistir la coincidencia, se considerar la siguiente letra del apellido materno, hasta corregir la coincidencia, por ejemplo: nombre: José Manuel Guizado Castillo, usuario: jguizadoc o mguizadoc.



	MUNICIPALIDAD DE VILLA EL SALVADOR	Año: 2022
	POLITICAS DE SEGURIDAD DE LA INFORMACION	Versión: 1.0
		Página: 10 de 72

- Cada servidor y locador es responsable de las actividades realizadas a través de sus cuentas de acceso de red, correo electrónico, sistemas de información asociados y sistemas de apoyo.

7.5.3. Gestión de Claves de Acceso

- La UDT de la Municipalidad Distrital de Villa El Salvador, establece contraseña de acceso como mecanismo de control, verificación y seguridad para el acceso lógico y físico en el uso de los recursos y servicio de TI para las unidades orgánicas de la Municipalidad Distrital de Villa El Salvador.
- Todo acceso a recursos y servicios de TI se realiza con una cuenta de usuario que es un identificador único compuesto por un usuario1 y contraseña.
- La contraseña está clasificada como información confidencial por lo cual no se debe compartir ni transferir, o mantener anotaciones de esta, ya sea en papeles o archivos digitales.
- Los servidores y locadores tienen prohibido usar una cuenta de usuario de otra persona o suplantar su identidad.
- Bajo la normativa de seguridad de la información, todo usuario está obligado a actualizar su contraseña de acceso en un determinado periodo.
- Las reglas que debe cumplir una contraseña segura son:
 - Debe ser como mínimo seis (6) hasta máximo de ocho (8) caracteres.
 - Debe ser entre letras, números y símbolos.
 - Debe contar con al menos una (1) letra mayúscula.
 - No contener nombre o apellido del usuario
- En caso de restaurar la contraseña de acceso, el usuario debe solicitar mediante el restablecimiento de contraseña a través de los documentos y formularios pertinentes, precisando el motivo de la solicitud y con autorización del encargado de la unidad orgánica al que pertenece.
- Referencia al Anexo Nro. 02 "Manual Interno de Gestión de Contraseñas".

7.5.4. Control de Acceso de Servicios Informáticos

- Todo usuario accederá a los recursos de TI, mediante la creación de cuentas genéricas, debidamente autorizadas y sustentadas por el encargado de la unidad orgánica, según corresponda.
- El acceso a los recursos de red, internos y externos, debe ser controlado por la UDT de la Municipalidad Distrital de Villa El Salvador, de manera que el servidor no comprometa la seguridad de los activos de información.
- La UDT de la Municipalidad Distrital de Villa El Salvador, supervisará los accesos a los recursos de TI de la Municipalidad, mediante herramienta de control y seguridad, para salvaguardar la confidencialidad, integridad y disponibilidad de la información, cuales están contemplados en el Anexo Nro.05 "Implementación de Directorio Activo y Administración de Usuarios en la Municipalidad Distrital de Villa El Salvador".
- El acceso a los sistemas operativos de las estaciones de trabajo de la Municipalidad Distrital de Villa El Salvador debe ser debidamente controlado por la UDT de la institución, a fin de evitar accesos no autorizados a recursos o información.
- Todo acceso y contraseña de usuarios para acceso al servicio informático deberá ser desactivadas después que la UGRH o la unidad orgánica que corresponda, comunique



	MUNICIPALIDAD DE VILLA EL SALVADOR	Año: 2022
	POLITICAS DE SEGURIDAD DE LA INFORMACION	Versión: 1.0
		Página: 11 de 72

el cese de las funciones de un servidor y locador, a la UDT de la Municipalidad Distrital de Villa El Salvador.

7.6. Políticas de Seguridad Física y Ambiental

7.6.1. Seguridad de las Áreas

- La UA de la Municipalidad Distrital de Villa El Salvador, encargado de la seguridad física de la Municipalidad Distrital de Villa El Salvador, debe verificar que los servidores porten visiblemente su fotocheck y locadores porten visiblemente su pase correspondiente, mientras dure su permanencia o visita en las instalaciones de la Entidad.
- La UDT de la Municipalidad Distrital de Villa El Salvador, debe implementar controles Biométricos al Centro de Datos para su debida protección.
- Toda persona externa a la Municipalidad Distrital de Villa El Salvador puede acceder a las áreas definidas, siempre que cuente con la autorización respectiva del jefe del órgano o unidad orgánica y debe estar siempre acompañado por un personal de la Entidad.
- La Municipalidad Distrital de Villa El Salvador a través de los Órganos u Unidades Orgánicas de acuerdo a su responsabilidad deben implementar medidas de protección contra amenazas externas y ambientales, debe incluir:
 - Detectores de humo, extintores
 - Sistema de alimentación ininterrumpida (UPS)
 - Sistema de puesta a Tierra
 - Sensores de aniego
 - Grupo Electrónico
- La UDT de la Municipalidad Distrital de Villa El Salvador debe contar con un ambiente adecuado para la conservación de medios magnéticos, equipos y dispositivos informáticos
- El Área de Archivo Central de la Municipalidad Distrital de Villa El Salvador debe contar con un ambiente apropiado para la conservación y protección de los documentos.
- Las oficinas o instalaciones donde se almacene o procese información confidencial (Centro de Datos, Archivo, entre otras) deben contar con acceso restringido y monitoreado con cámaras de videovigilancia. El ingreso y salida de los servidores y locadores autorizados debe ser registrado por las Unidades Orgánicas responsables de dichos ambientes y, de ser el caso, emplear mecanismos biométricos.

7.6.2. Seguridad de los Equipos Informáticos

- La UDT de la Municipalidad Distrital de Villa El Salvador, debe asegurar el funcionamiento de los equipos del centro de datos a través del respaldo de energía eléctrica, ante la pérdida del servicio de suministro eléctrico.
- UDT de la Municipalidad Distrital de Villa El Salvador, debe mantener un programa de mantenimiento preventivo de los equipos de Tecnologías de información y de los sistemas de acondicionamiento de temperatura, humedad y filtrado de aire, sistemas de energía ininterrumpida (UPS) y sistemas de detección y extinción de fuego del Data Center, a fin de garantizar la continuidad de los servicios.
- La UDT de la Municipalidad Distrital de Villa El Salvador, será el encargado de clasificar, asignar y distribuir los equipos informáticos a las unidades orgánicas.



	MUNICIPALIDAD DE VILLA EL SALVADOR	Año: 2022
	POLITICAS DE SEGURIDAD DE LA INFORMACION	Versión: 1.0
		Página: 12 de 72

- Solo el servidor y locador de soporte técnico de la UDT podrá realizar la apertura de los equipos informáticos.
- Cuando un recurso de TI es retirado, reubicado o reasignado, se debe efectuar las acciones apropiadas de control de inventario técnico para asegurar que los registros respectivos se encuentren actualizados
- La UDT de la Municipalidad Distrital de Villa El Salvador, debe definir el procedimiento de borrado seguro en los equipos de cómputo y demás positivos, una vez que pase a estado de Baja.

7.7. Políticas de Infraestructura del Centro de Datos “DATACENTER”

El Centro de Datos es considerado una instalación crítica por almacenar y procesar información sensible e importante para la Municipalidad Distrital de Villa El Salvador.

7.7.1. Gestión de Acceso

- El acceso al Centro de Datos está permitido sólo al personal técnico autorizado de UDT de la Municipalidad Distrital de Villa El Salvador. El ingreso y salida es previa identificación dactilar (huella) o mediante uso de llave en el dispositivo de acceso.
- El acceso a los servidores de la Municipalidad Distrital de Villa El Salvador ya sea cuando la consola de administración local o una consulta administración remota es monitoreado por el personal autorizado por la UDT.

7.7.2. Infraestructura

- El Centro de Datos debe mantener la temperatura del aire acondicionado entre 15 a 21 grados Celsius para evitar daños en los equipos o en peores casos incidentes relacionados con fuego.
- Contar con medios de seguridad como extintores, sistema de alarma y contra incendios.
- Cualquier mantenimiento efectuado en las áreas continuas al Centro de Datos que impliquen uso de químicos o agentes emisores de humo, polvo, gases o cualquier otra sustancia que afecte las alarmas del Centro de Datos, debe ser comunicado y coordinado con la UDT de la Municipalidad Distrital de Villa El Salvador, a fin de prevenir alguna alteración del Centro de Datos.

7.8. Política de Seguridad de las Operaciones

7.8.1. Procedimiento Operativos Documentados

- La UDT de la Municipalidad Distrital de Villa El Salvador, debe documentar procesamientos operativos, estableciendo las responsabilidades y los recursos utilizados para su ejecución, asimismo, estos deberán estar a disposición de los servidores autorizados.
- La UDT de la Municipalidad Distrital de Villa El Salvador, debe mantener un registro de control de cambios de los sistemas, equipos de comunicación, bases de datos, equipos de cómputo y perfiles de acceso, a través de la implementación de acciones y procedimientos orientados a asegurar que todo cambio siga un proceso planificado que incluya responsabilidades y canales de comunicación, identificación de los recursos comprometidos, pruebas de comprobación, controles de seguridad, reversión en caso de fallas y análisis de impacto.
- La UDT de la Municipalidad Distrital de Villa El Salvador, debe definir y documentar procedimientos para pases de desarrollo a producción, asimismo, el entorno de pruebas



	MUNICIPALIDAD DE VILLA EL SALVADOR	Año: 2022
	POLITICAS DE SEGURIDAD DE LA INFORMACION	Versión: 1.0
		Página: 13 de 72

debe ser en lo posible, igual al ambiente de producción en lo referido a recursos de Tecnologías de información.

- La UDT de La Municipalidad Distrital De Villa El Salvador debe mantener un registro de incidentes de virus o ataque informático y otros ataques consideramos graves o de alta importancia, incluyendo las acciones realizadas para su atenciones y solución.

7.8.2. Protección contra Software Malicioso

- La UDT de la Municipalidad Distrital de Villa El Salvador, debe adoptar las medidas necesarias para la prevención, detección y eliminación de código malicioso (malware) a nivel de servidores de red, computadoras portátiles, estaciones de trabajo.
- La UDT de la Municipalidad Distrital de Villa El Salvador, debe asegurar que todas las estaciones de trabajo estén protegidas con el antivirus corporativo y que éste se encuentre actualizado.
- La UDT de la Municipalidad Distrital de Villa El Salvador, es el responsable de la renovación de licencias de softwares en los servidores, equipos de cómputo, comunicaciones o seguridad perimetral, implementadas en la Entidad.

7.8.3. Gestión en Soporte Técnico.

- La UDT de la Municipalidad Distrital de Villa El Salvador, debe procurar mantener y garantizar los servicios disponibles de acuerdo a las condiciones y acuerdos de niveles de servicio especificados en el Anexo Nro. 03 *"Implementación de Sistema de Mesa de Ayuda"*.
- Las atenciones de soporte técnico y las acciones realizadas para la resolución de incidentes y problemas deber ser registradas y centralizadas en el manual de procedimiento, Anexo Nro. 03 *"Implementación de Sistema de Mesa de Ayuda"* de la UDT de la Municipalidad Distrital de Villa El Salvador".
- Está terminantemente prohibido utilizar recursos de la Municipalidad Distrital de Villa El Salvador, para realizar acciones de soporte técnico a equipos particulares del servidor y locador que laboran en la Entidad.
- La UDT de la Municipalidad Distrital de Villa El Salvador, es responsable de la provisión de los recursos y servicios de TI que se requieran para el funcionamiento del Portal Institucional de la Entidad. Siendo responsabilidad de los órganos pertinentes la operación y el suministro de información para su actualización.
- Todo servidor y locador de la Municipalidad Distrital de Villa El Salvador, no debe realizar instalación de software en los equipos informáticos, esta actividad es parte de las funciones de la UDT.
- La UDT de la Municipalidad Distrital de Villa El Salvador, debe tener actualizada la documentación de roles detallados y tareas para cada personal involucrado en la ejecución del plan de continuidad de servicios de TI.
- La Gerencia Municipal debe proporcionar a la UDT de la Municipalidad Distrital de Villa El Salvador, las herramientas y equipos tecnológicos adecuados para el mantener la información protegida ante cualquier riesgo ocasionado en la Entidad.



7.8.4. Respaldo de la Información

- La UDT de la Municipalidad Distrital de Villa El Salvador, es la unidad orgánica encargada de gestionar el respaldo de la información en formato digital, así como base de datos y archivos almacenados en la unidad compartida, el cual se establece en el

	MUNICIPALIDAD DE VILLA EL SALVADOR	Año: 2022
	POLITICAS DE SEGURIDAD DE LA INFORMACION	Versión: 1.0
		Página: 14 de 72

Manual Interno Anexo Nro.04 "Procesos de Copias de Base de Datos de Sistemas e Información General de la Municipalidad Distrital de Villa El Salvador".

- La UDT de la Municipalidad Distrital de Villa El Salvador a través del Oficial de Seguridad de la Información o quien haga a sus veces, debe normalizar los requisitos necesarios para la protección ambiental y física de las copias de respaldo.
- Las copias diarias de respaldo de la información son conservadas por 90 días de antigüedad.
- La UDT de la Municipalidad Distrital de Villa El Salvador debe mantener el registro actualizado de las operaciones de gestión de respaldo y recuperación, así como de las fallas que pudieran presentarse y las soluciones realizadas, a través del personal de soporte técnico.
- La UDT de la Municipalidad Distrital de Villa El Salvador, realizará un cronograma para pruebas periódicas (mínimo anual) de recuperación del respaldo, para asegurar que son confiables cuando sean necesario.
- La UDT de la Municipalidad Distrital de Villa El Salvador, debe estimar anticipadamente la cantidad necesaria de medios magnéticos requeridos para efectuar las copias de respaldo, en caso de no contar con ello, solicitar su oportuna adquisición.
- Todo servidor y locador que detecten vulnerabilidad o debilidad que pueda afectar la seguridad de la información, recursos o servicios de TI, debe comunicarlo al Oficial de Seguridad de la Información o quien haga de sus veces, mediante el registro de incidencias, Anexo 01 "Registro de Incidencias de Seguridad de la Información".
- La UDT de la Municipalidad Distrital de Villa El Salvador, debe revisar periódicamente la vigencia tecnológica de los equipos y software utilizados para el respaldo y recuperación de la información.
- La UDT de la Municipalidad Distrital de Villa El Salvador, debe realizar el análisis de vulnerabilidad técnicas de los sistemas de información, más prioritarios y programar las acciones necesarias para prevenir o mitigar los riesgos identificados en el análisis.
- La UDT de la Municipalidad Distrital de Villa El Salvador, debe dar cumplimiento que el usuario que, al ausentarse de su estación de trabajo, debe bloquear la pantalla o en estado de Suspendido. Y todo dispositivo de almacenamiento de datos como CD, USB, Disco Duro Externo, y medios removibles en general, deben ser retirados del escritorio para evitar el acceso no autorizado a los mismos.
- La UDT de la Municipalidad Distrital de Villa El Salvador, debe hacer cumplir que, usuario debe mantener su escritorio limpio (pantallas, tableros, etc) libre de información, propia de la Entidad, que pueda estar al alcance del personal no autorizado.
- La UDT de la Municipalidad Distrital de Villa El Salvador, debe implementar controles de protección de privacidad de los datos personales almacenados en los registros de eventos de los sistemas de información.

7.9. Políticas de Seguridad de las Comunicaciones

La UDT de la Municipalidad Distrital de Villa El Salvador con soporte del Oficial de Seguridad de la Información o quien haga de sus veces, debe implementar mecanismos de control y procedimientos necesarios para proveer la disponibilidad de las redes de datos y de los servicios que dependen de ellas; asimismo, que disponga de controles de seguridad que protejan la integridad y la confidencialidad de la información que se transporta a través de dichas redes de datos. El control de acceso a los



	MUNICIPALIDAD DE VILLA EL SALVADOR	Año: 2022
	POLITICAS DE SEGURIDAD DE LA INFORMACION	Versión: 1.0
		Página: 15 de 72

recursos de la red se establece en el *Anexo Nro.05 "Implementación de Directorio Activo y Administración de Usuarios en la Municipalidad Distrital de Villa el salvador"*

7.9.1. Gestión de seguridad sobre los servicios de la red

- El encargado de cada órgano o unidad orgánica de la Municipalidad Distrital de Villa El Salvador, es el responsable de solicitar acceso a los servicios de la red, mediante los documentos y formulario pertinente.
- Los servicios de correo electrónico, red de datos y acceso a internet, son administrados por la UDT de la Municipalidad Distrital de Villa El Salvador y están a disposición de los servidores y locadores autorizado por la unidad orgánica al que pertenece, para el desempeño de sus funciones.
- Las credenciales electrónicas (cuentas, nombres de usuario, claves de acceso y todo mecanismo de identificación por medios informáticos) para el acceso a los recursos y servicios de TI disponibles, deben ser otorgados al personal específicamente autorizado para dicho acceso. Las responsabilidades del uso de las credenciales otorgadas son estrictamente individuales y no son transferibles.
- La UDT de la Municipalidad Distrital de Villa El Salvador, es el encargado de efectuar la desactivación de la cuenta de correo electrónico institucional por algún uso indebido que transgreda lo establecido en el presente documento.
- Los accesos a las páginas de internet serán monitoreados por la UDT de la Municipalidad Distrital de Villa El Salvador y ante cualquier violación de acceso se debe informar al funcionario de la unidad orgánica correspondiente mediante correo electrónico.
- Durante el empleo de los servicios de red e internet se deben evitar prácticas o usos inapropiados que pudieran poner en riesgo la confidencialidad, integridad y disponibilidad de la información utilizada en la Municipalidad Distrital de Villa El Salvador.
- Cada servidor y locador es responsable por la información que se trasmite desde la cuenta de correo electrónico institucional asignado por la Municipalidad Distrital de Villa El Salvador.
- Todo servidor y locador que reciba correos electrónicos sospechosos y/o origen desconocido, debe comunicar a la UDT a través del Oficial de Seguridad de la Información o quien haga de sus veces de la Municipalidad Distrital de Villa El Salvador, para fines correspondientes.
- No es permitida la instalación de puntos de acceso de redes inalámbricas con conexión a los recursos de TI de la Municipalidad Distrital de Vila El Salvador.
- No Utilizar la cuenta de correo electrónico suministrada por la UDT de la Municipalidad Distrital de Villa El Salvador, para asuntos personales o de otra índole que no sea parte de sus funciones en la Municipalidad.
- Todo servidor y locador que necesite acceso a redes sociales, capacitación online u otros servicios aparte de correo electrónico, deberá solicitarlo mediante documento y formulario correspondiente, indicando el tiempo de acceso y justificación del requerimiento, con la autorización del encargado de la unidad orgánica al que corresponda.
- La UDT de la Municipalidad Distrital de Villa El Salvador, debe verificar que los cables que transportan datos se encuentren debidamente protegidos contra la interceptación, inferencia o posibles daños.



	MUNICIPALIDAD DE VILLA EL SALVADOR	Año: 2022
	POLITICAS DE SEGURIDAD DE LA INFORMACION	Versión: 1.0
		Página: 16 de 72

7.10. Política de Adquisición, desarrollo y mantenimiento de los Sistemas de información.

- 7.10.1.** La UDT de la Municipalidad Distrital de Villa El Salvador, debe aprobar un procedimiento para la adquisición, desarrollo y mantenimiento de los sistemas
- 7.10.2.** Todo desarrollo y/o mantenimiento de sistemas debe ser documentado, con la finalidad de que servidor y locador no relacionada con ellas en el Municipalidad Distrital de Villa El Salvador, ejecuten las actividades con facilidad
- 7.10.3.** La UDT de la Municipalidad Distrital de Villa El Salvador, debe definir un procedimiento que incluya controles de seguridad durante las etapas de análisis y diseño de los sistemas.
- 7.10.4.** La UDT de la Municipalidad Distrital de Villa El Salvador, debe implementar controles de seguridad apropiados en los sistemas utilizadas por la Entidad para validar los datos de entrada, el procesamiento interno y los datos de salida.
- 7.10.5.** Todo sistema desarrollado por los servidores de la UDT de la Municipalidad Distrital de Villa El Salvador, debe satisfacer los requisitos de seguridad definidos para el desarrollo y mantenimiento de los sistemas. En el caso de los locadores, el desarrollo de los sistemas debe constar en el respectivo contrato de prestación de servicios.
- 7.10.6.** La UDT de la Municipalidad Distrital de Villa El Salvador, debe verificar que los acuerdos sobre materia informática a suscribir con locadores, incluyan cláusulas relativas a la cesión de derechos y confidencialidad de la información, para el resguardo de la propiedad intelectual de la Municipalidad Distrital de Villa El Salvador.
- 7.10.7.** El desarrollo y/o mantenimiento de los sistemas de información implementados en la Municipalidad Distrital de Villa El Salvador, se requerirán a través de requerimientos funciones, los cuales deben ser formalmente solicitados por los distintos órganos y unidades orgánicas, teniendo en consideración las normas y guías establecidas para dichos fines.
- 7.10.8.** Las actividades de capacitación sobre el funcionamiento de un aplicativo informático relacionado deben realizarse antes de su puesta en producción, en coordinación con la unidad orgánica solicitante, definiendo las condiciones mínimas para su realización
- 7.10.9.** La UDT de la Municipalidad Distrital de Villa El Salvador, podrá recurrir al desarrollo de sistemas de la información por "outsourcing", cuando no cuente con el recurso humano y/o tecnológico necesario, para llevar a cabo los desarrollos de forma interna, además cuando otros factores como el tiempo no lo permitan. Dichas solicitudes deberán ser formalmente presentadas por las gerencias, subgerencias y áreas, en forma escrita e indicando los requerimientos generales por cubrir.
- 7.10.10.** El control y monitoreo del avance del proyecto de sistemas de información por "outsourcing" estará a cargo de la UDT de la Municipalidad Distrital de Villa El Salvador, además estará pendiente que la empresa contratada brinde la capacitación a sus funcionarios y servidores en administración, uso y mantenimiento del nuevo sistema de información.
- 7.10.11.** El pase a producción debe ser realizado exclusivamente por el servidor y locador autorizada por la UDT de la Municipalidad Distrital de Villa El Salvador, quien lleva un control de los pases efectuados y/o actualizaciones de los sistemas en un registro o bitácora.

7.11. Política de relación con los Proveedores

- 7.11.1.** Todo proveedor que brinde servicios a la Municipalidad Distrital de Villa El Salvador, debe suscribir un acuerdo de confidencialidad, la misma que será parte del contrato de prestación de servicios como anexo.
- 7.11.2.** Los proveedores sólo podrán desarrollar para la Municipalidad Distrital de Villa El Salvador, aquellas actividades cubiertas bajo el correspondiente contrato u orden de servicios.
- 7.11.3.** El proveedor debe proporcionar los datos completos de la persona de contacto, quien se encarga de recibir todo tipo de directivas de seguridad de la información.

	MUNICIPALIDAD DE VILLA EL SALVADOR	Año: 2022
	POLITICAS DE SEGURIDAD DE LA INFORMACION	Versión: 1.0
		Página: 17 de 72

- 7.11.4. El proveedor proporciona mensualmente, mientras dure la vigencia del contrato, la relación de personas, perfiles, funciones y responsabilidades asociadas al servicio previsto, e informa puntualmente de cualquier cambio (alta, baja, sustitución o cambio de funciones o responsabilidades) que se produzca en dicha relación.
- 7.11.5. Todo proveedor que tenga acceso a la información del Municipalidad Distrital de Villa El Salvador, en ejecución de un contrato u orden de prestación de servicios, debe considerar que dicha información, es confidencial y sujeto a la Ley de Protección de Datos Personales.
- 7.11.6. Ningún proveedor puede utilizar la información del Municipalidad Distrital de Villa El Salvador para beneficio propio si no, únicamente puede ser utilizada para los fines específicamente indicados en el contrato u orden de prestación de servicios. Toda información proporcionada por la Municipalidad Distrital de Villa El Salvador, sigue siendo de propiedad de esta última.
- 7.11.7. Los recursos que la Municipalidad Distrital de Villa El Salvador pone a disposición del proveedor, independientemente del tipo que sean, (informáticos, datos, software, redes, sistemas de comunicación, etc.) están exclusivamente destinados para cumplir con las obligaciones y propósito para los que fueron proporcionados.
- 7.11.8. El proveedor debe notificar a la UDT de la Municipalidad Distrital de Villa El Salvador, cualquier incidencia que se detecte y que afecte o pueda afectar a la seguridad de la Información de la Entidad.

8. Responsabilidades

8.1. Encargados

- 8.1.1. **Oficina de Secretaria General:** Deberá informar a la UDT de la Municipalidad Distrital de Villa El Salvador mediante resolución, cuando finalice el contrato de funcionarios de la entidad, además definir e implementar los controles de acceso físico.
- 8.1.2. **UDT:** Es responsable del uso de la política de TIC como herramienta de gestión y definir los estándares para que la entidad de cumplimiento a la misma. Poner a disposición los recursos necesarios para que las políticas de TIC de la Municipalidad Distrital de Villa El Salvador, se lleven a cabo de acuerdo con los establecido en la presente política. Designar el personal idóneo para apoyar la implementación de la presente política. Cualquier requerimiento de modificación de las políticas debe ser dirigido a la UDT de la Municipalidad Distrital de Villa El Salvador, quien será el encargado de mantener actualizado la política de TIC.
- 8.1.3. **Las Unidades Orgánicas:** Están obligadas a conocer y difundir las políticas y lineamientos descritos en el presente documento y velar por su cumplimiento. Además, debe comunicar a la UDT de la Municipalidad Distrital de Villa El Salvador la culminación del contrato del locador y proveedor para desactivar los accesos que le fueron asignados para su desempeño laboral.
- 8.1.4. **Los funcionarios de las unidades orgánicas:** deberán informar las sugerencias, modificaciones o cambios que consideren necesarias al presente Documento, con el objeto de precisar alcances, mejorar y/o modificar políticas que incidan en la eficacia de las mismas. Estas propuestas serán comunicadas a la UDT de la Municipalidad Distrital de Villa El Salvador para su evaluación y aprobación.
- 8.1.5. **Oficial de Seguridad de la Información:** Velar que el cumplimiento de la presente política se lleve a cabo de acuerdo con los lineamientos de seguridad establecidos por la Municipalidad.
- 8.1.6. **Unidad de Gestión de Recursos Humanos:** Deberán informar a la UDT de la Municipalidad Distrital de Villa El Salvador, cuando finalice el contrato del personal CAS.



	MUNICIPALIDAD DE VILLA EL SALVADOR	Año: 2022
	POLITICAS DE SEGURIDAD DE LA INFORMACION	Versión: 1.0
		Página: 18 de 72

8.2. Violación a las Políticas

La infracción o incumplimiento de las políticas sobre tecnologías de la información, ser notificado al órgano o unidad orgánica correspondiente, así como, a la UDT de la Municipalidad Distrital de Villa El Salvador, a fin de que procedan a realizar las acciones administrativas correspondientes.

8.3. Revisiones Periódicas

Cualquier cambio en el ordenamiento legal vigente, en la estrategia institucional o en los procesos y funciones de la Municipalidad que afecte al propósito del presente manual, suscitara una actualización de su contenido con el fin de adaptarlo a las nuevas circunstancias.

9. Anexos

- 9.1. Anexo Nro.01 "Registro de Incidencias de Seguridad de la Información"
- 9.2. Anexo Nro.02 "Manual Interno de Gestión de Contraseñas"
- 9.3. Anexo Nro.03 "Implementación de Sistema de Ayuda"
- 9.4. Anexo Nro.04 "Procesos de Copias de Base de Datos de Sistemas e Información General de la Municipalidad Distrital de Villa El Salvador"
- 9.5. Anexo Nro.05 "Implementación de Directorio Activo y Administrativo de Usuarios en la Municipalidad Distrital de Villa El Salvador"
- 9.6. Anexo Nro.06 "Manual Interno de Recuperación de Información del SIAF"



ANEXOS

Anexo Nro01 : “Registro de Incidencias de Seguridad de la Información”

	MUNICIPALIDAD DISTRICTAL DE VILLA EL SALVADOR	FORMULARIO NRO 8 REGISTRO DE INCIDENCIA DE SEGURIDAD DE INFORMACION	VERSIÓN: 1.0 PÁGINA: 1
(Debe ser llenado letra imprenta)			
DATOS DE QUIEN REPORTE EL INCIDENTE			
Nombres:		Apellidos:	
DNI o Nro. Pasaporte:		Móvil:	
<i>Si es personal de la Municipalidad</i>		<i>Si no es personal de la Municipalidad</i>	
Unidad Orgánica		Nombre de la Empresa (contratista) / Servicio Contratado	
Cargo:			
Correo Institucional:		Anexo:	
INFORMACION SOBRE EL INCIDENTE			
Fecha:		Hora:	
De la siguiente lista seleccione y marque con una "X" las opciones que considere se encuentre relacionadas con el incidente reportado			
N°	PELIGRO / ASPECTO / AMENAZA	MARCA	
1	DESASTRE NATURAL: incendio, inundación, rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras.		
2	DE ORIGEN INDUSTRIAL: Incendio, inundación, contaminación mecánica, contaminación electromecánica, avería de origen físico o lógico, corte del suministro eléctrico (accidental o deliberado), condiciones inadecuadas de temperatura o humedad, fallo de servicios o comunicaciones, interrupción de otros servicios y suministros esenciales, degradación de los soportes de almacenamiento de información (disco duro, cd, dvd, usb), emanaciones electromagnéticas (interceptación de señales parásitas comprometedoras), otros (explosiones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas, accidentes de tráfico)		
3	ERRORES Y FALLOS NO INTENCIONADOS Errores de los usuarios, errores del administrador, errores de monitorización (log), errores de configuración, deficiencias en la organización, difusión de software dañino (virus, spyware, gusanos, troyanos, etc), errores de reencaminamiento, errores de secuencia, escapes de información, alteración de la información, destrucción de información, fugas de información, vulnerabilidades de los programas (software), errores de mantenimiento o actualización de programas, errores de mantenimiento o actualización de equipos, caída del sistema por agotamiento de recursos: indisponibilidad del personal		
4	ATAQUES INTENCIONADOS: Manipulación de los registros de actividad (log), manipulación de la configuración, suplantación de la identidad del usuario, abuso de privilegios de acceso, uso no previsto, uso de software dañino (virus, spyware, gusanos, troyanos, etc), reencaminamiento de mensajes, iteración de la secuencia, acceso no autorizado, análisis de tráfico, repudio, interceptación de información (escucha pasiva), modificación deliberada de información, destrucción de información, divulgación de información (divulgación, geolocalización, copia ilegal de software), manipulación de programas, manipulación de equipos (sabotaje de hardware), denegación del servicio (saturación del sistema informático), robo (soporte o documentos y/o hardware), ataque destructivo (destrucción de hardware o de soportes).		




Unidad de Desarrollo Tecnológico



 <p>MUNICIPALIDAD DISTRITAL DE VILLA EL SALVADOR</p>	FORMULARIO NRO 8 REGISTRO DE INCIDENCIA DE SEGURIDAD DE INFORMACION	VERSIÓN: 1.0 PÁGINA: 2
---	--	---------------------------

5 OTROS (especificar):

DESCRIPCION DEL INCIDENTE

A continuación, describa el incidente que está reportando, ¿según detalle siguiente?

¿Qué Ocurrió?

¿Como Ocurrió?

¿Por qué Ocurrió?

¿Qué Componentes se vieron afectados? (Describa el impacto generado)

Firma

Fecha de Envío de Reporte

TÉRMINOS:

- El presente documento se puede enviar en forma física a Unidad de Desarrollo Tecnológico o por email en archivo PDF al correo institucional del Subgerente de la Unidad de Desarrollo Tecnológico



Unidad de Desarrollo Tecnológico

	MUNICIPALIDAD DE VILLA EL SALVADOR	Año: 2022
	POLITICAS DE SEGURIDAD DE LA INFORMACION	Versión: 1.0
		Página: 21 de 72

Anexo Nro.02 : “Manual Interno de Gestión de Contraseñas”

1. Creación de Contraseña

- Los usuarios accederán a los recursos de TI, mediante la creación de cuentas genéricas, debidamente autorizadas y sustentadas por el jefe de la unidad orgánica, según corresponda.
- Toda cuenta de usuario utilizara la letra inicial del primer nombre seguido por el apellido paterno más la letra inicial del apellido materno. En caso de coincidir el nombre y apellidos con los de otro usuario, se deber considerar, además, la letra inicial del segundo nombre. De persistir la coincidencia, se considerar la siguiente letra del apellido materno, hasta corregir la coincidencia. Ej. Personal: Juan Luis Perez Torres, usuario: jperezt o lperezt.
- La UDT de la Municipalidad Distrital de Villa El Salvador, establece contraseña de acceso como mecanismo de control, verificación y seguridad para el acceso lógico y físico en el uso de los recursos y servicio de TI para las unidades orgánicas de la MVES.
- La UDT de la Municipalidad Distrital de Villa El Salvador, determina el periodo de vigencia de las contraseñas, siendo obligación del usuario su cambio respectivo, bajo responsabilidad. Tener en cuenta lo siguiente:
 - Debe tener al menos 6 a 7 caracteres (letras, números o símbolos)
 - Debe tener al menos una letra mayúscula.
 - Debe tener al menos una letra minúscula.
 - Debe tener al menos un número.
 - No debe contener nombre o apellidos de usuario
 - La contraseña no puede ser alguna se haya usado previamente (para los casos de cambio de contraseña periódica)
 - Ejm: Sist3m@5
- La cuenta del usuario y contraseña es entregada en sobre cerrado y sellado.



- La contraseña de acceso a los servicios de TI es de uso personal e intransferible.
- Todos los acceso y contraseñas de usuarios para el uso de sistema de información de la Municipalidad, deberán ser desactivadas o cambiados después que un funcionario, locador o empleado cese prestar sus servicios.

2. Recuperación de Contraseña

- La unidad orgánica debe enviar un memorando solicitando el Restablecimiento de la Contraseña a la UDT de la Municipalidad Distrital de Villa El Salvador.
- Llenar los datos del usuario al formulario N° 03 solicitando Reestablecer Contraseña, indicando el tipo de cuenta, cargo, unidad orgánica, jefe inmediato y motivo de la solicitud, debidamente Firmado.





	MUNICIPALIDAD DISTRITAL DE VILLA EL SALVADOR	FORMULARIO Nro. 3	VERSIÓN: 4.0
		REESTABLECER CONTRASEÑA	PÁGINA: 1 de 1

(Debe ser llenado por el Usuario y con letra imprenta)

Referencia al Memorando Nro.						
Fecha de la Solicitud: / / (dd/mm/aaaa)						
TIPO DE CUENTA A REESTABLECER CONTRASEÑA (marcar solo una opción)						
Marcar con X	<input type="checkbox"/> Sistema Informático			<input type="checkbox"/> Correo Institucional	<input type="checkbox"/> Usuario PC (red munives)	<input type="checkbox"/> VPN usuario (CAS/Fijo)
	<i>Si marco Sistema Informático, llenar: (marcar una opción)</i>			<i>Si marco Usuario PC o VPN, llenar:</i>		
	<input type="checkbox"/> SIGAMEF	<input type="checkbox"/> SITRADO (actual)	<input type="checkbox"/> RENTAS GESMUN	Cod. Patrimonial CPU:		
	<input type="checkbox"/> RUOS	<input type="checkbox"/> SIAF MVES	<input type="checkbox"/> SIAF Mancomunidad			
	<input type="checkbox"/> RENTAS (antigua)	<input type="checkbox"/> SIGAVES (antigua)	<input type="checkbox"/> SISCOMP. (Sist. Comprob.)			
<input type="checkbox"/> SIGAVES	<input type="checkbox"/> OTROS					
Especificar (si marco otros):						
DATOS DEL USUARIO						
Cuenta o Usuario (login):		DNI o Pasaporte:				
Nombres y Apellidos:						
Motivo:			Régimen Laboral:			
Sede:			Unidad Orgánica:			
Jefe Inmediato:						

TÉRMINOS DE RESPONSABILIDADES:

- **El responsable de la Unidad Orgánica:** Es el único autorizado a solicitar la recuperación de contraseña de las cuentas de usuarios. Estará obligado a comunicar a la Unidad de Desarrollo Tecnológico (UDT), siempre que se sucedan cambios en las cuentas de los usuarios habilitados.
- **El usuario será el único responsable:** Responsable en el manejo que se le dé a la información a la que tiene acceso. Atender y aplicar el acuerdo de Confidencialidad y las Recomendaciones para la Manipulación y Almacenamiento de Información que se mencionan a continuación se le enviara con la relación permisos asignados, si no está de acuerdo con algún o algunos de los términos definidos por favor solicite la desactivación de su usuario.



Firma y sello Jefe Inmediato

Firma del Usuario.

Unidad de Desarrollo Tecnológico



	MUNICIPALIDAD DE VILLA EL SALVADOR	Año: 2022
	POLITICAS DE SEGURIDAD DE LA INFORMACION	Versión: 1.0
		Página: 23 de 72

Anexo Nro.03 : “Implementación de Sistema de Ayuda”

1. INTRODUCCION

Debido a la carencia de control de incidencias informáticas en la Municipalidad de Villa El Salvador, este documento presenta la propuesta de implementar la Mesa de Ayuda mediante el sistema de gestión de incidencias basado en un software libre, para solucionar la problemática, mejorar los procesos de asistencia técnica, facilitar el trabajo realizado por los técnicos y aportar en el desarrollo tecnológico de la Municipalidad.

La Mesa de Ayuda permite examinar el problema que presente cualquier usuario a través de un ticket o solicitud en el que aparecen todos los detalles del requerimiento. Luego de que el problema haya sido notificado, la mesa de ayuda trabajara en la gestión de todos los tickets o solicitudes para que el equipo de soporte pueda dar seguimiento y solución a los problemas lo más pronto y efesivamente posible.

Las políticas de gestión que se aplique en un proceso de centralización de fallas lideradas por el área de UDT de la Municipalidad Distrital de Villa El Salvador, llamado mesa de ayuda, dará como resultado la asistencia oportuna y la mejora del servicio a atención eficaz, teniendo como base la metodología ITIL v3 la cual cuenta con énfasis en el servicio y contiene las buenas prácticas para la tecnología de la información.

2. OBJETIVOS

2.1. Objetivo General

Implementar una herramienta de Mesa de Ayuda, que permita brindar asistencia y soporte técnico a las incidencias, requerimientos, problemas o accesos relacionados a los Servicios de TI que brinda específicamente la UDT, a los usuarios internos y externos de la Municipalidad de Villa el Salvador.

2.2. Objetivo Especifico

- Definir las necesidades y requerimientos en la UDT de la Municipalidad Distrital de Villa El Salvador para la implementación de la mesa de ayuda.
- Diseñar y ejecutar un protocolo de pruebas que permita verificar la funcionalidad de la mesa de ayuda que satisfaga las necesidades del proyecto.
- Realizar un diagnóstico que permita cuantificar en el tiempo, el desempeño de los procesos implantados (o por implantar) y controlar la ejecución de las actividades definidas para los procesos de incidentes y solicitudes de cambios, de acuerdo con los niveles de servicio establecidos.
- Proponer la estrategia para la optimización de los servicios brindados por parte de la mesa de ayuda bajo los lineamientos de la Metodología ITIL v3, las normas ISO/IEC 2000:2011.



3. ALCANCE

El alcance de esta implementación de atención de Mesa de Ayuda con sistema de gestión de incidencias, es que considere de forma transversal los procesos mediante los procesos de la fase de Operación del Servicio, Gestión de Peticiones, Gestión de Incidencias, Gestión de Problemas y Gestión de Accesos. El procedimiento aplica a todos los actores que desempeñan diferentes roles dentro de la Municipalidad Distrital de Villa el

	MUNICIPALIDAD DE VILLA EL SALVADOR	Año: 2022
	POLITICAS DE SEGURIDAD DE LA INFORMACION	Versión: 1.0
		Página: 24 de 72

Salvador, inicia con el reporte de incidencias y requerimientos y finaliza con el cierre de las mismas y con la generación de estadísticas de operación de la mesa de ayuda de la UDT.

4. RESPONSABLE

- **Usuario:** Es la persona que solicita un servicio y/o comunica algún problema o incidencia, por medio de línea telefónica, correo electrónico o ingresar el ticket por la aplicación de mesa de ayuda (HelpDesk Munives).
- **Coordinador de Mesa de ayuda:** Es el encargado de recepcionar todas las solicitudes de soporte que se generan y asignar los servicios, dependiendo el caso. Chequear el tiempo se cierre de las incidencias, con la finalidad de asistir el soporte en tiempo establecido. También brinda apoyo por la aplicación, por teléfono o en forma remota. Genera reportes semanales de la cantidad de incidencias ingresados, estados, tiempo de cierre, estadísticas e informes personalizados según requerimiento.
- **Soporte Técnico:** Encargado de gestionar la mesa de ayuda, realizar visitas para dar el diagnóstico y la correcta solución al problema registrado, cerrando así el ciclo de la incidencia. Para luego documentar y finalizar el soporte.
- **El Profesional de Soporte Especializado:** Es el responsable de garantizar, hacer seguimiento a los incidentes o solicitudes escalados a proveedores, y confirmar si la solución brindada es acorde a la solicitud realizada por el usuario. El personal profesional / técnico de Sistemas: Será el encargado de gestionar los servicios solicitados a través de los medios establecidos en la actividad 2, a su vez es el responsable de garantizar la gestión de todos los incidentes y requerimientos reportados a la mesa de ayuda, generar análisis y reportes que lleven a la mejora continua de los procedimientos de resolución de incidentes y solicitudes.

5. REFERENCIA Y BASES LEGALES

- Ley No 27658, Ley de Marco de la Modernización del Estado, En proceso de modernización en sus diferentes instancias, dependencias, entidades, organizaciones y procedimientos, con la finalidad de mejorar y descentralizar la gestión pública al servicio del ciudadano.
- NTP-ISO/IEC 20000-1:2012 Tecnología de la Información, Normas que especifican los requisitos para que un proveedor del servicio pueda planificar, establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGS. Los requisitos intervienen en el diseño, transición, entrega y mejora de servicios para cumplir con los requisitos del servicio.
- ITIL v4.0, Revisión al marco de trabajo más ampliamente aceptado a nivel mundial para la Administración de Servicios de TI (ITSM). Se compone de una guía comprensiva de como adoptar y adaptar las mejores prácticas de gestión.
- Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
- Decreto Supremo N° 004-2013-PCM, Decreto Supremo que aprueba la Política Nacional de Modernización de la Gestión Pública.



	MUNICIPALIDAD DE VILLA EL SALVADOR	Año: 2022
	POLITICAS DE SEGURIDAD DE LA INFORMACION	Versión: 1.0
		Página: 25 de 72

- Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición”, en todas las entidades integrantes del Sistema Nacional de Informática

6. CONDICIONES GENERALES

La solicitud de servicio de tecnologías de información será gestionada a través del aplicativo de mesa de ayuda que permite visualizar la trazabilidad de todas las solicitudes.

Cuando las solicitudes de servicios tecnológicos se encuentren vinculadas al Banco de datos Personales de la Municipalidad se debe considerar lo siguiente:

- El/la Oficial de Seguridad de la Información notifica, mediante correo institucional, a el/la Oficial de Datos Personales, el estado de los incidentes.
- El/La Oficial de Seguridad de la Información revisa con el/la Oficial de Datos Personales los aspectos legales que los incidentes puedan ocasionar a la Municipalidad.

Los Niveles de Atención a la Solicitud de servicio a la tecnología de la información están determinado por tres niveles de atención:

- Nivel 1: Personal que brinda asistencia de primer nivel, mediante vía telefónica o asistencia remota.
- Nivel 2: Personal especialistas encargadas de brindar soporte técnico, mediante vía telefónica o asistencia física (acercarse a la unidad orgánica)
- Nivel 3: Personal externo (proveedores) que brinda soporte de requerimientos que no fueron solucionados en nivel 1 y 2.

Los medios de atención que el usuario dispondrá para solicitar la atención de servicio de la tecnología de la información.

- Sistema Gestión de incidencias: la unidad usuaria está obligada de registrar las incidencias o solicitudes mediante un ticket de servicio en el programa de Gestión de incidencias.
- Documento memorando: utilizado para solicitar requerimientos que necesite la firma y sello del jefe de la Unidad Orgánica.
- Teléfono: el anexo 212 es el canal de atención más utilizado por los usuarios, si el anexo se encuentra atendiendo otra solicitud, automáticamente nuestra central telefónica deriva la llamada al anexo del taller de UDT de la Municipalidad Distrital de Villa El Salvador.



	MUNICIPALIDAD DE VILLA EL SALVADOR	Año: 2022
	POLITICAS DE SEGURIDAD DE LA INFORMACION	Versión: 1.0
		Pagina: 26 de 72

Equipo de Soporte

Agente	Cargo	Función
Subgerente	Subgerente	Gestión Administrativa
Asistente	Secretaria	Tramite Documentario
Soporte	HelpDesk	Registrar y Asignar tickets
Programador 1	Soporte	Coordinador de Desarrollo de Software Institucional (nivel 2)
Programador 2	Analista Desarrollador	Personal de Desarrollo 1 de software (nivel 2)
Programador 3	Desarrollador	Personal de Desarrollo 2 de software (nivel 2)
Analista	Analista Funcional	Personal de Análisis de software (nivel2)
Soporte 1	Encargado Soporte	Coordinador para la Asistencia 1 de Networking e Infraestructura
Soporte 2	Administrador de Red y Comunicaciones	Asistente Técnico 3 de Networking
Soporte 3	Encargado Soporte	Asistente Técnico 2 de equipos informáticos



7. DEFINICIONES

- **Sistema de gestión de mesa de ayuda:** Aplicativo informático que permite el registro y seguimiento de las solicitudes de servicios de tecnologías de la información.
- **Incidente:** Resultado de fallos o errores en la infraestructura TI, es decir es cualquier evento que no forma parte del desarrollo habitual del servicio y que causa, o puede causar una interrupción del mismo.
- **Requerimiento:** Solicitud realizada por el usuario, frente a una solicitud específica y está sujeto de ser evaluado y priorizado su tiempo de atención de acuerdo a los acuerdos de niveles de servicio.
- **Modelo de atención:** Documento donde se encuentran las tareas a ejecutarse de acuerdo a una programación para cada solicitud de servicio.
- **Solicitud de servicio:** Solicitud que hace un/a usuario/a reportando incidentes, requerimientos, cambios o peticiones registrados en ticket de atención.
- **Usuario/a:** Servidor/a civil, proveedor, locador/a contratado/a, practicante pre profesional, practicante profesional, que tenga vínculo laboral o contractual con la Entidad; o, se encuentre en alguna modalidad formativa, según corresponda; y, use habitualmente el hardware y software brindados por el Municipalidad.
- **UDT:** Unidad de Desarrollo Tecnológico, órgano de apoyo en la Municipalidad Distrital de Villa El Salvador.





- **Ticket:** Es un archivo o dato numérico contenido y generado en el sistema de seguimiento que contiene información acerca de intervenciones a los incidentes reportados por un usuario final a la mesa de ayuda de soporte técnico.
- **Estados de solicitud de servicio (ticket)**
 - Abierto: solicitud o ticket registrado por el usuario en el sistema de gestión de incidencias, pendiente en asignar y solucionar.
 - Asignado: solicitud o ticket asignado a un agente de soporte para su atención.
 - Resuelto: solicitud atendida y/o solucionado por soporte.
 - Cerrado: solución de solicitud validado y cierre de servicio.

8. POLITICAS DE OPERACIÓN.

- Los servicios de soporte técnico solo se proporcionarán a equipos, periféricos y servicios que son parte de la Entidad.
- Atender las peticiones por cola de atención y prioridad
- Todas las solicitudes para el otorgamiento de Servicios de Soporte se levantarán vía telefónica, correo electrónico, memorando o por la aplicación de mesa de ayuda.
- Todo ticket creado y/o registrado en la herramienta de repositorio debe cumplir con un ciclo de estados, desde la solicitud del requerimiento hasta su cierre a satisfacción.
- Funciones Operativas de la UDT.
 - Atender y dar soporte tecnológico a los requerimientos e Incidencias de TI.
 - Atención a las solicitudes de instalación y configuración de equipos informáticos.
 - Proporcionar equipos informáticos a las unidades usuarias. (Anexo3)
 - Asistir a la atención de incidencias operativas, instalación y capacitación en los sistemas de información de la Municipalidad.
 - Atender y resolver las consultas, incidencias y problemas de operatividad de los sistemas de información y de apoyo.
 - Realizar mantenimiento preventivo y correctivo a los equipos de cómputo. (Manual de Mantenimiento preventivo y correctivo de equipos informáticos)
 - Brindar acceso a la Red de Datos y correo electrónico institucional. (Anexo1)
 - Habilitar puntos de acceso a la red de comunicación interna. (Anexo1)
 - Atender el servicio a la instalación y configuración a los teléfonos IP.
 - Proporcionar acceso a internet y configuración según perfil de usuario.
 - Instalar y configurar en los equipos asignados los sistemas de información actual y de apoyo, así como herramientas o software autorizados.
 - Brindar mantenimiento de Sistemas de Información municipal actuales, así como desarrollar nuevos sistemas.
 - Brindar mantenimiento de Sistemas de información de apoyo actuales, así como desarrollar nuevas aplicaciones.
 - Brindar mantenimiento de los portales Web y desarrollar nuevas funcionalidades.
 - Brindar respaldo y servicio de restauración de la información de los sistemas de información en producción.
 - Elaborar informes técnicos y TDR para servicios relacionados con Tecnologías de la Información.
 - Elaborar de normas o estándares de Tecnología de la Información para el acceso y uso adecuado de los servicios tecnológicos de la MVES.
 - Brindar servicio de capacitación en el uso herramientas de ofimática u otros sistemas de información.
- **No se atenderán casos de ofimática pues son competencias básicas de cada funcionario, servidor y locador.**





9. DESCRICIONES DE PROCEDIMIENTO

9.1. Tabla Explicativa Del Procedimiento de Mesa de Ayuda.

ACTIVIDADES			EJECUTOR
N.º	ACTIVIDAD	DESCRIPCION	RESPONSABLE
1	Inicio Recibir la solicitud de servicio de TI	Recepción de solicitud, según los siguiente: Si la solicitud se realiza por correo, vía telefónica o memorando, se ingresa al sistema de gestión de mesa de ayuda, va a la actividad N.º 2. Si la solicitud se realiza por el sistema de gestión de mesa de ayuda, va a la actividad N.º 3.	Operador HelpDesk
2	Identificar el tipo de servicio	Identifica el tipo de solicitud y prioridad. En caso se trate de una solicitud de servicios de TI , va la actividad N.º 3. En caso se trate de un incidente o problema , se procede de acuerdo al instructivo de atención de incidentes y problemas de TI, y va a la actividad N.º 6.	Operador HelpDesk
3	Clasificar y verificar la aprobación de la solicitud de servicio de TI	Clasifica y verifica si la solicitud de servicio de TI requiere aprobación para su atención: ¿Se acepta la solicitud? Si: va a la actividad N.º 4 No: va a la actividad N.º 6 Cambia el estado de la solicitud a "en espera" .	Coordinador de soporte y desarrollo.
4	Enviar la solicitud para aceptación	Deriva solicitud, mediante correo, para su aceptación conforme a los servicios de Ti estipulados por UDT En caso que acepte el coordinador del área va a la actividad N.º 5	Operador HelpDesk
5	verificar y aceptar la solicitud	Verifica y acepta la solicitud ¿la solicitud es viable a solucionar? Si: va a la actividad N.º 6 No: va a la actividad N.º 12	Coordinador de Soporte y Desarrollo
6	Asignar la solicitud	Asigna la solicitud a el/la Especialista de UDT para su atención. Cambia el estado de la solicitud a "asignado" .	Operador HelpDesk
7	Revisar y atender la solicitud	Examinar la solicitud asignada y la atiende conforme al Instructivo de atención de solicitud de servicios de TI. ¿La solicitud es atendida? Si: va a la actividad N.º 8 No: va a la actividad N.º 6	Operador de Soporte y Desarrollo
8	Actualizar el estado de la solicitud	Actualiza el estado de la solicitud con el resultado de las acciones realizadas. Cambia el estado de la solicitud a "Resuelto" . ¿solicitud fue ingresada por memorando?	Operador de soporte y Desarrollo





		Si: va a la actividad N.º 9 No: va a la actividad N.º 10	
9	Generar memorando	Generar memorando como respuesta a la solicitud Derivar documento a la unidad orgánica usuaria o solicitante	Secretaria de UDT
10	Validar solución	validar que la solicitud fue atendida, vía llamada telefónica. ¿Conformidad del usuario? Si: va a la actividad N.º 11 No: va a la actividad N.º 7	Coordinador de Soporte y Desarrollo
11	Cerrar el registro de solicitud	Procede al cierre del registro de la solicitud y generar el reporte de gestión de solicitudes. Cambia el estado de la solicitud a " cerrado ".	Coordinador de Soporte
12	Identificar y coordinar acciones de mejora	Identificar y coordina, mediante correo institucional, con el/la jefe de soporte técnico las posibles soluciones a implementar.	Operador de Soporte y Desarrollo
13	Evalúa y aprueba	Evalúa y aprueba mediante correo institucional, la viabilidad de las soluciones. ¿Es viable? Si: va a la actividad N.º 14 No: va a la actividad N.º 12	Subgerente UDT
14	Implementar y revisar	Implementa las acciones para la mejora del servicio y revisar los resultados.	Operador de Soporte y Desarrollo
15	Verificar las mejoras de servicios	Valida las acciones implementadas. ¿Es Conforme? Si: va a la actividad N.º 16 No: va a la actividad N.º 13	Operador de Soporte y Desarrollo
16	Comunicar y registrar la acción implementada para mejora. Fin del Procedimiento	Comunica, mediante correo institucional, a el/la jefe de UTI la acción implementada de mejora,	Operador de Soporte y Desarrollo



9.2. Diagrama De Flujo Del Procedimiento de Mesa de Ayuda (Anexo05)



	MUNICIPALIDAD DE VILLA EL SALVADOR	Año: 2022
	POLITICAS DE SEGURIDAD DE LA INFORMACION	Versión: 1.0
		Página: 30 de 72

10. REGISTRO DE SOLICITUD O INCIDENCIA EN EL SISTEMA DE MESA DE AYUDA.

- Registrar ticket para solicitar servicio y/o comunicar incidencias en el sistema mesa de ayuda, mediante el link Sistema de Soporte (munives.gob.pe) y digitar la clave de acceso brindado por UDT.
- Usuario debe iniciar sesión para ingresar un nuevo Ticket; donde permitirá ingresar la incidencia o solicitud de servicio. Link de acceso : Sistema de Soporte (munives.gob.pe).

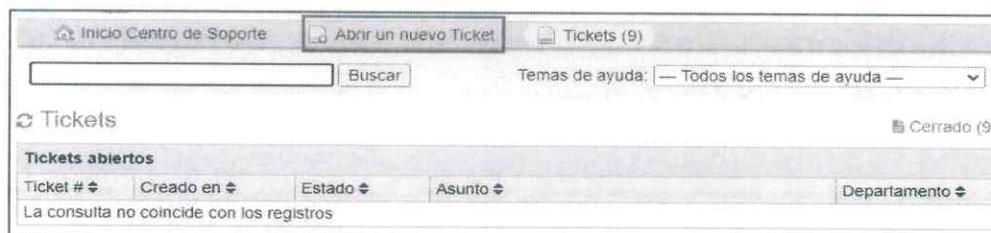


- Ingresar el nombre de usuario y la clave





- Para registrar un ticket de incidencia o solicitud, primero debe elegir el Tema de Ayuda.






Email: registrocivil@munives.gob.pe
Cliente: Área de Registro Civil

Temas de ayuda

- Seleccione un tema de ayuda —
- Seleccione un tema de ayuda —
- Asistencia Técnica / Ajustes/Cambios en SigaVes
- Asistencia Técnica / Atasco de Hoja
- Asistencia Técnica / Bloqueo / Lentitud
- Asistencia Técnica / Conectar impresora a PC**
- Asistencia Técnica / Conexión a la Red
- Asistencia Técnica / CPU No Prende
- Asistencia Técnica / CPU Reinicia
- Asistencia Técnica / Falla de Anexo
- Asistencia Técnica / Mensaje de Error
- Asistencia Técnica / Monitor no Prende
- Asistencia Técnica / No abre correo Institucional
- Asistencia Técnica / No hay Internet
- Asistencia Técnica / No Imprime
- Asistencia Técnica / Otros
- Instalar/Reinstalar Programas / Rentas - Caja
- Instalar/Reinstalar Programas / Rentas Antiguo
- Instalar/Reinstalar Programas / Siat Mancomunidad
- Instalar/Reinstalar Programas / Siat Mves
- Instalar/Reinstalar Programas / SIGAVES

- Completar el ticket con los siguientes datos y adjuntar imagen o documento (opcional).

Email: registrocivil@munives.gob.pe
Cliente: Área de Registro Civil

Temas de ayuda
Asistencia Técnica / Conectar impresora a PC

Detalles de la incidencia
Por favor, describa su problema o requerimiento.

Asunto
Conexión a impresora

Detalle de la incidencia
Código Patrimonial del equipo afectado:
Usuario: Nombre del personal que informa la incidencia o solicita un servicio
Información Adicional: (puede detener de las anomalías)

Adjuntar archivos: foto.jpg

- Así se visualiza el Ticket registrado por el usuario. (ticket en estado abierto).

Conexión a Impresora #001143

Información básica del ticket
Estado del Ticket: Abierto
Departamento: Help Desk UDT
Creado en: 3/11/21 14:20

Información de usuario
Nombre: Área De Registro Civil
Email: registrocivil@munives.gob.pe
Teléfono:

Área de Registro Civil publicado 3/11/21 14:20

Código Patrimonial del equipo afectado:
Usuario: Nombre del personal que informa la incidencia o solicita un servicio
Información Adicional: (puede detener de las anomalías)

Adjuntar archivos: foto.jpg



- Lista de tickets abiertos por usuario (pendientes por responder).

Área de Registro Civil | perfil | Tickets (11) - Cerrar sesión

Inicio Centro de Soporte | Abrir un nuevo Ticket | Tickets (11)

Temas de ayuda: — Todos los temas de ayuda —

Tickets | Abrir (2) | Cerrado (9)

Mostrando 1 - 2 de 2 Tickets abiertos

Ticket #	Creado en	Estado	Asunto	Departamento
000143	3/11/21	Abierto	Conexión a impresora	Help Desk UDT
000137	3/11/21	Abierto	Revisión Impresora Memo 177-2021	Help Desk UDT

Página: [1]



- El operador de Mesa de Ayuda, accede al sistema para asignar y priorizar ticket, Link de acceso : [osTicket :: Inicio de sesión de agente \(munives.gob.pe\)](https://osTicket::Inicio de sesión de agente (munives.gob.pe))



- Así se visualiza el ticket ingresado por usuario (prioridad normal por defecto).

Open

Ticket de Atención	Fecha	Asunto	Unidad Usuaría	Prioridad	Asignar a
<input type="checkbox"/> 000143	3/11/21 14:27	Conexion a Impresora #	Área de Registro Civil	Normal	
<input type="checkbox"/> 000141	3/11/21 14:06	conexion de una impresora	Subgerencia Recaudación Control y Ejecutora Coactiva	Normal	Macpierre Carbonero Condezo

Ticket #000143

Conexion a Impresora

Estado: Abierto
 Prioridad: Normal
 Departamento: Help Desk UDT
 Creado en: 3/11/21 14:27

Usuario: Área de Registro Civil (11) (Gestionar Colaboradores)
 Email: registrocivil@munives.gob.pe
 Fuente: Web - (205.45.91.111)

Asignado a: -- Sin asignar --
 Plan de SLA: Ninguno
 Fecha de Vencimiento: -- Vacío --

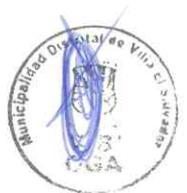
Temas de ayuda: Asistencia Técnica / Conectar Impresora a PC
 Último mensaje: 3/11/21 14:27
 Última respuesta:

Hilo del Ticket (1) Tareas

Área de Registro Civil publicado 3/11/21 14:27

Tipo y código patrimonial del equipo informático
 Usuario (nombre del personal que informa el incidente o solicita un servicio):
 Información Adicional (breve detalle de las anomalías)





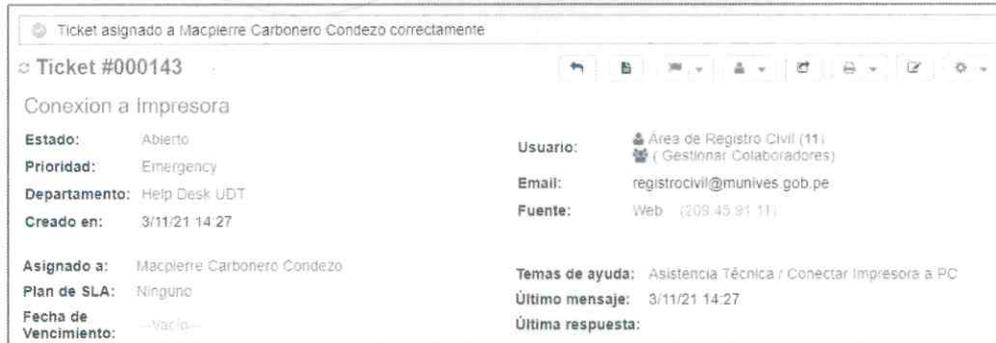
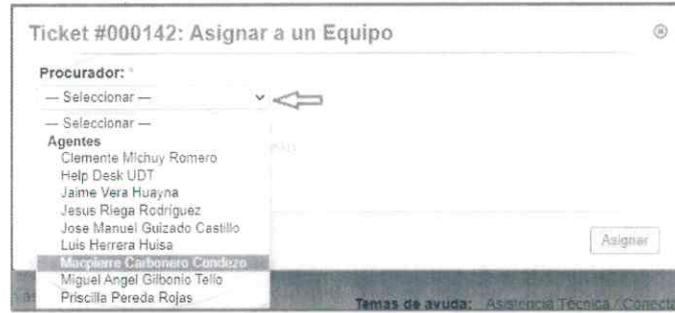
- Operador Helpdesk procede a priorizar, asignar agente y fecha límite de atención.

Ticket #000142: actualizar Nivel Prioridad

Nivel Prioridad:
 Emergency
 -- Seleccionar --
 Low
 Normal
 High
 Emergency

Cancelar actualizar





- Lista de Tickets de abiertos (*pendientes*) en perfil de Operador HelpDesk

Ticket	Fecha	Asunto	Unidad Usaria	Prioridad	Asignado a
000143	3/11/21 14:31	Conexion a impresora #	Área de Registro Civil	Emergency	Macpierre Carbonero Condezo
000137	3/11/21 13:53	Revisión impresora Memo 177-2021 #	Área de Registro Civil	High	Clemente Michuy Romero
000144	3/11/21 14:37	no pueden ingresar al meet	Unidad de Tesorería	Normal	Macpierre Carbonero Condezo
000141	3/11/21 14:06	conexion de una impresora	Subgerencia Recaudación Control y Ejecutora Coactiva	Normal	Macpierre Carbonero Condezo
000140	3/11/21 13:51	el teclado no funciona	Unidad Planeamiento Estratégico Modernización y Programación de Inversiones	Normal	Macpierre Carbonero Condezo
000138	3/11/21 10:26	instalar un equipo en ODI	Órgano de Control Institucional	Normal	Macpierre Carbonero Condezo
000125	28/10/21 14:07	problemas con el acceso a internet	Unidad de Tesorería	Normal	Jesus Riega Rodriguez
000049	4/10/21 11:41	Alerta en correo, se queda sin espacio	Unidad de Desarrollo Tecnológico	Normal	Priscilla Pereda Rojas



- Lista de Tickets de abiertos (*pendientes*) en perfil de Operador HelpDesk

Ticket	Fecha	Asunto	Unidad Usaria	Prioridad	Asignado a
000143	3/11/21 14:31	Conexion a impresora #	Área de Registro Civil	Emergency	Macpierre Carbonero Condezo
000137	3/11/21 13:53	Revisión impresora Memo 177-2021 #	Área de Registro Civil	High	Clemente Michuy Romero
000144	3/11/21 14:37	no pueden ingresar al meet	Unidad de Tesorería	Normal	Macpierre Carbonero Condezo
000141	3/11/21 14:06	conexion de una impresora	Subgerencia Recaudación Control y Ejecutora Coactiva	Normal	Macpierre Carbonero Condezo
000140	3/11/21 13:51	el teclado no funciona	Unidad Planeamiento Estratégico Modernización y Programación de Inversiones	Normal	Macpierre Carbonero Condezo
000138	3/11/21 10:26	instalar un equipo en ODI	Órgano de Control Institucional	Normal	Macpierre Carbonero Condezo
000125	28/10/21 14:07	problemas con el acceso a internet	Unidad de Tesorería	Normal	Jesus Riega Rodriguez
000049	4/10/21 11:41	Alerta en correo, se queda sin espacio	Unidad de Desarrollo Tecnológico	Normal	Priscilla Pereda Rojas



- El Agente ingresa a atender los tickets asignados. Link de acceso : [osTicket :: Inicio de sesi3n de agente \(munives.gob.pe\)](https://osTicket::Inicio%20de%20sesi3n%20de%20agente%20(munives.gob.pe))

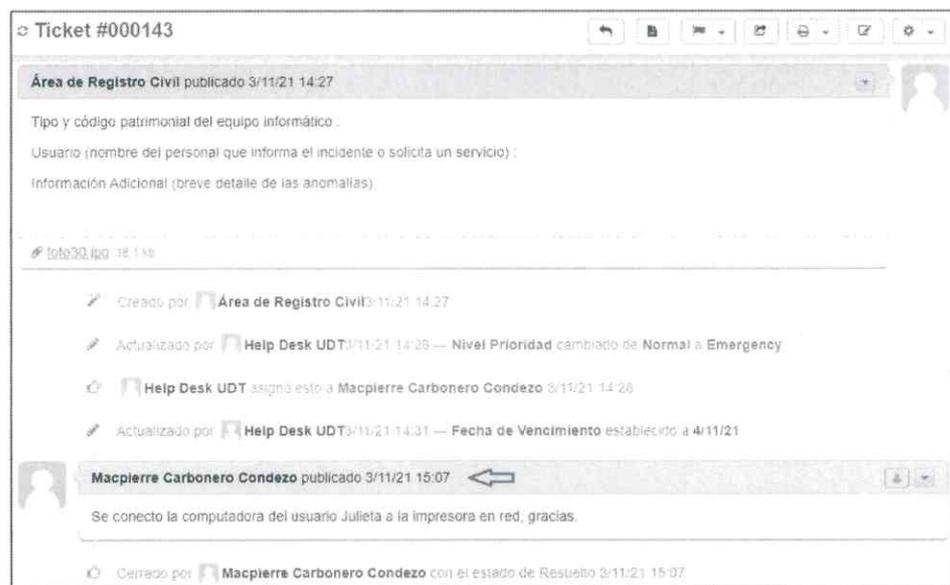


- Lista de tickets pendientes por Agente. Ejm : MacPierre



Ticket	Fecha	Asunto	Unidad Usuarria	Prioridad	Area
000143	3/11/21 14:31	Conexi3n a Impresora	Área de Registro Civil	Emergency	Help Desk UDT
000140	3/11/21 13:51	el teclado no funciona	Unidad Planeamiento Estratégico Modernizaci3n y Programaci3n de Inversiones	Normal	Help Desk UDT
000139	3/11/21 10:26	instalar un equipo en OCI	Órgano de Control Institucional	Normal	Help Desk UDT

- Agente atiende y responde Ticket.



Ticket #000143

Área de Registro Civil publicado 3/11/21 14:27

Tipo y código patrimonial del equipo informático :
 Usuario (nombre del personal que informa el incidente o solicita un servicio) :
 Información Adicional (breve detalle de las anomalías)

📎 foto30.jpg 18.1 kb

- ✔ Creado por **Área de Registro Civil** 3/11/21 14:27
- ✎ Actualizado por **Help Desk UDT** 3/11/21 14:28 — Nivel Prioridad cambiado de Normal a Emergency
- 👤 **Help Desk UDT** asignó esto a **MacPierre Carbonero Condezo** 3/11/21 14:28
- ✎ Actualizado por **Help Desk UDT** 3/11/21 14:31 — Fecha de Vencimiento establecido a 4/11/21

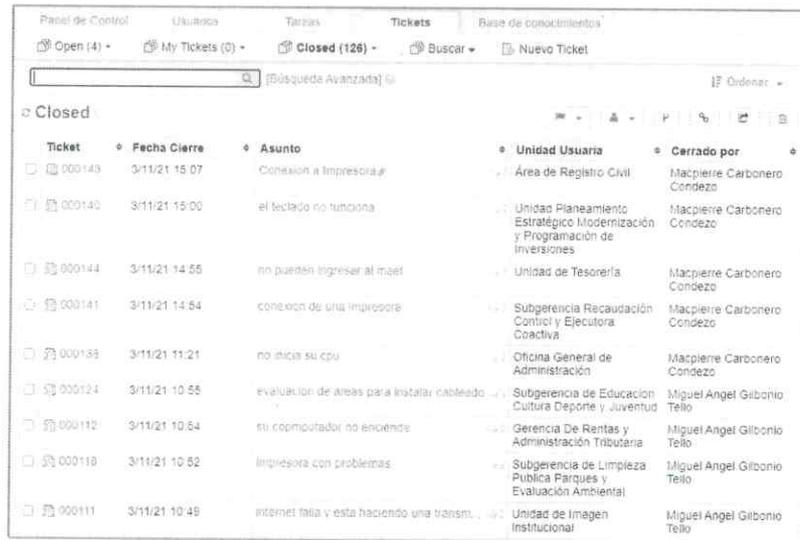
MacPierre Carbonero Condezo publicado 3/11/21 15:07

Se conecto la computadora del usuario Julieta a la impresora en red, gracias.

🔒 Cerrado por **MacPierre Carbonero Condezo** con el estado de Resuelto 3/11/21 15:07

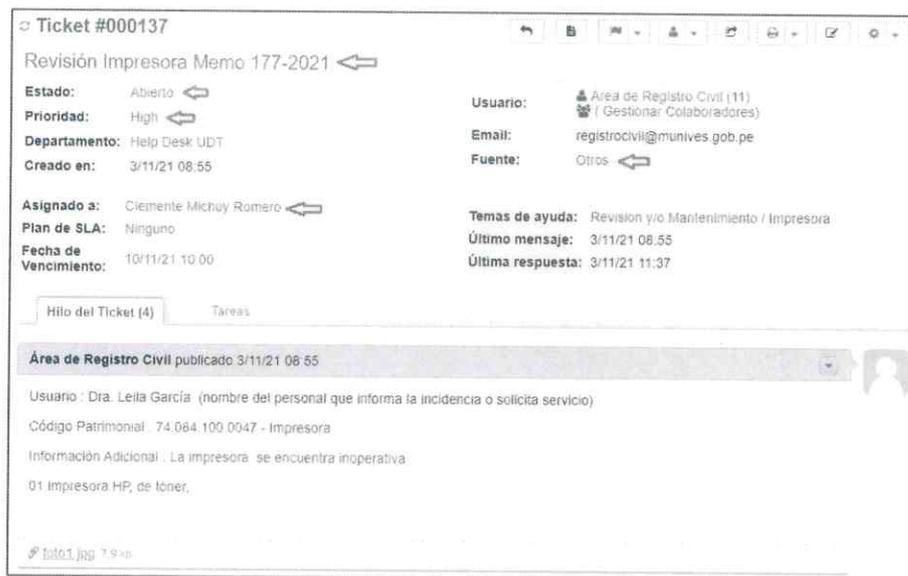


- Lista de Tickets cerrados (*resueltos*), en el panel de Operador Helpdesk



Ticket	Fecha Cierre	Asunto	Unidad Usuaria	Cerrado por
000143	3/11/21 15:07	Conexion a Impresora	Área de Registro Civil	Macpierre Carbonero Condezo
000140	3/11/21 15:00	el teclado no funciona	Unidad Planeamiento Estratégico Modernización y Programación de Inversiones	Macpierre Carbonero Condezo
000144	3/11/21 14:55	no pueden ingresar al maet	Unidad de Tesorería	Macpierre Carbonero Condezo
000141	3/11/21 14:54	conexion de una impresora	Subgerencia Recaudación Control y Ejecutora Coactiva	Macpierre Carbonero Condezo
000158	3/11/21 11:21	no inicia su cpu	Oficina General de Administración	Macpierre Carbonero Condezo
000124	3/11/21 10:55	evaluacion de areas para instalar cableado	Subgerencia de Educacion Cultura Deporte y Juventud	Miguel Angel Gilbonio Tello
000112	3/11/21 10:54	su computador no enciende	Gerencia De Rentas y Administración Tributaria	Miguel Angel Gilbonio Tello
000118	3/11/21 10:52	Impresora con problemas	Subgerencia de Limpieza Publica Parques y Evaluación Ambiental	Miguel Angel Gilbonio Tello
000111	3/11/21 10:48	internet falla y esta haciendo una transm...	Unidad de Imagen Institucional	Miguel Angel Gilbonio Tello

- Registrar ticket para solicitar servicio y/o comunicar incidencias por medio de memorando, correo o teléfono, el operador de helpdesk ingresar al sistema para ingresar el ticket de atención.
 - El usuario solicita un servicio por medio de memorando, el operador helpdesk registra, prioriza y asigna el ticket.



Ticket #000137

Revisión Impresora Memo 177-2021

Estado: Abierto
 Prioridad: High
 Departamento: Help Desk UDT
 Creado en: 3/11/21 08:55

Usuario: Área de Registro Civil (11)
 Email: registrocivil@municipal.gov.pe
 Fuente: Otros

Asignado a: Clemente Michuy Romero
 Plan de SLA: Ninguno
 Fecha de Vencimiento: 10/11/21 10:00

Temas de ayuda: Revisión y/o Mantenimiento / Impresora
 Último mensaje: 3/11/21 08:55
 Última respuesta: 3/11/21 11:37

Hilo del Ticket (4)

Área de Registro Civil publicado 3/11/21 08:55

Usuario: Dra. Leila García (nombre del personal que informa la incidencia o solicita servicio)

Código Patrimonial: 74.084.109.0047 - Impresora

Información Adicional: La impresora se encuentra inoperativa

01 Impresora HP, de tóner,



- El usuario informa la incidencia o solicita un servicio por medio teléfono, el operador helpdesk registra, prioriza y asigna el ticket.

Ticket #000147

NO PUEDE IMPRIMIR

Estado: Abierto	Usuario: Catastro y Control Urbano Subgerencia de Obras Privadas
Prioridad: Normal	(9) Gestionar Colaboradores
Departamento: Help Desk UDT	Email: udt@munives.gob.pe
Creado en: 4/11/21 08:47	Fuente: Teléfono
Asignado a: Macpierre Carbonero Condezo	Temas de ayuda: Asistencia Técnica
Plan de SLA: Ninguno	Último mensaje: 4/11/21 08:47
Fecha de Vencimiento: 6/11/21 10:27	Última respuesta:

Hilo del Ticket (1) Tareas

Catastro y Control Urbano Subgerencia de Obras Privadas publicado 4/11/21 08:47

USUARIO MARLE NO PUEDE IMPRIMIR

CR. 100 por Help Desk UDT 4/11/21 08:47

Help Desk UDT asigno esto a Macpierre Carbonero Condezo 4/11/21 08:47

Actualizado por Help Desk UDT 4/11/21 09:27 — Fecha de Vencimiento establecido a 6/11/21

- Estadística de tickets por tema de ayuda

Estadísticas

Las estadísticas de los Tickets se organizan por departamento, ayuda, tema y agente

Rango: September 30, 2021 - October 30, 2021 (America/Lima)

Temas de ayuda	Abierto	Asignado	Atrasado	Cerrado	Reabierto	Borrado	Tiempo de Servicio	Tiempo de Respuesta
Asistencia Técnica	30	34	0	27	0	0	11.2	23.8
Asistencia Técnica / CPU No Prende	3	3	0	2	0	0	17.0	73.8
Asistencia Técnica / No imprime	5	7	0	5	0	0	16.2	18.2
Asistencia Técnica / No hay Internet	2	1	0	2	0	0	18.7	11.0
Asistencia Técnica / Conexion a la Red	7	7	0	7	0	0	20.1	12.1
Asistencia Técnica / Mensaje de Error	1	1	0	1	0	0	0.0	0.0
Instalar/Reinstalar Programas	1	1	0	1	0	0	1.0	1.0
Instalar/Reinstalar Programas / Rentas - Caja	1	2	0	1	0	0	48.0	48.0
Instalar/Reinstalar Programas / Siat Mves	2	2	0	2	0	0	0.0	0.0
Asistencia Técnica / Otros	19	20	1	21	0	0	34.9	16.6
Revision y/o Mantenimiento / impresora	1	1	0	0	0	0	0.0	193.0
Revision y/o Mantenimiento / Laptop	1	2	0	1	0	0	76.0	76.0
Asistencia Técnica / Conectar Impresora a PC	7	8	0	7	0	0	13.7	13.8
Asistencia Técnica / Ajustes/Cambios en SigaVes	7	7	0	6	1	1	0.0	0.0
Asistencia Técnica / No abre correo institucional	1	1	0	1	0	0	6.0	6.0
Asistencia Técnica / Fallo de Anexo	1	1	0	1	0	0	3.0	3.0

Exportar



11. ANEXOS

11.1. Anexo 1: Formulario Alta o Baja de Cuenta de Usuario

	MUNICIPALIDAD DISTRITAL DE VILLA EL SALVADOR	FORMULARIO NRO 1 ALTA O BAJA DE CUENTA DE USUARIO	VERSIÓN: 5.0 PÁGINA: 1
(Debe ser llenado por el Jefe Inmediato y con letra impresa)			
Referencia al Memorando Nro.			
Fecha de la Solicitud: / / (dd/mm/aaaa)			
ACCION (marcar solo una opción)			
Solicito (marcar con X)	<input type="checkbox"/> Crear	<input type="checkbox"/> Desactivar	<input type="checkbox"/> Reactivar
	<input type="checkbox"/> Regularizar	<input type="checkbox"/> Modificar	
TIPO DE CUENTA (marcar solo una opción)			
<input type="checkbox"/> Usuario PC (red Munives)	<input type="checkbox"/> Correo Institucional	<input type="checkbox"/> Sistema Informático	<input type="checkbox"/> VPN usuario (CAS/Fijo)
			<input type="checkbox"/> Acceso Remoto (Anydesk/Teamviewer)
Si marco Regularizar (Correo o Usuario PC), llenar:		Si marco Sistema, llenar: (marcar una opción)	
Si marco Teletrabajo (VPN) o Acceso Remoto, llenar:			
Nombre de Cuenta (del usuario anterior):	<input type="checkbox"/> SIGAMEF	<input type="checkbox"/> SITRADO (actual)	Cod. Patrimonial (CPU):
	<input type="checkbox"/> RENTAS GEMUN	<input type="checkbox"/> RUOS	Motivo:
	<input type="checkbox"/> SIAF MVES	<input type="checkbox"/> SIAF Mancom.	Mac: IP:
Apellidos y Nombres (del usuario anterior):	<input type="checkbox"/> RENTAS (antiguo)	<input type="checkbox"/> SISTRADO (antiguo)	Entidad Solicitante:
	<input type="checkbox"/> SIGAVES	<input type="checkbox"/> SISCOMP (Sist.Comp.)	
	<input type="checkbox"/> OTROS		Periodo:
Especificar (Si marco otros)			
Nro. De Perfil	(solicitar Perfil)	Centro de Costo (Si marco SIAF o SIGAVES)	
DATOS DEL USUARIO			
Apellidos:	Nombre:		
Cargo:	DNI:		
Anexo o Celular:	Régimen Laboral:		
Correo Institucional:			
DATOS DEL AREA SOLICITANTE			
Sede:	Unidad Orgánica:		
Jefe Inmediato:	Teléf. o Anexo:		
TÉRMINOS DE RESPONSABILIDADES:			
<ul style="list-style-type: none"> El responsable de la Unidad Orgánica: Es el único autorizado a solicitar la habilitación y cancelación de las cuentas de usuarios. Estará obligado a comunicar a la Unidad de Desarrollo Tecnológico (UDT), los cambios que surjan en las cuentas de los usuarios habilitados. En caso de reemplazar personal por cese de funciones es necesario enviar otro formulario con los datos de dicho usuario antiguo para desactivar todas las cuentas registradas. El usuario será el único responsable en el manejo que le dé a la información a la que tiene acceso. Está obligado a atender y aplicar El acuerdo de Confidencialidad (Anexo1), las Recomendaciones para la Manipulación y Almacenamiento de Información que se mencionan y Perfil de Usuario (Anexo2) que contiene los procesos asignados. Si no está de acuerdo con algún o algunos de los términos definidos por favor solicite la desactivación de su usuario. Si por algún motivo se le ha asignado alguna opción del Sistema que no le corresponde, comunicar inmediatamente para proceder a la modificación del Perfil correspondiente. Este formato debe adjuntar El Perfil de Usuario y el Acuerdo de Confidencialidad firmado. 			
Firma y Sello del Jefe Inmediato		Firma del Usuario.	
		 	
Unidad de Desarrollo Tecnológico			



MUNICIPALIDAD DE VILLA EL SALVADOR	Año: 2022
POLITICAS DE SEGURIDAD DE LA INFORMACION	Versión: 1.0
	Página: 38 de 72



MUNICIPALIDAD
DISTRITAL DE
VILLA EL
SALVADOR

FORMULARIO NRO 1
ALTA O BAJA DE CUENTA DE USUARIO

VERSIÓN: 4.0
PÁGINA: 2 de 11

ACUERDO DE CONFIDENCIALIDAD

Anexo 01

(Debe ser llenado por el Usuario y con letra imprenta)

Yo, _____, identificado(a), con DNI Nro. _____, en mi condición de usuario de los sistemas y/o herramientas dispuestas por la **Municipalidad de Villa El Salvador**, entiendo y acepto las condiciones, compromisos, derechos y deberes, relacionados en el presente documento denominado **Acuerdo de Confidencialidad**, dado que tengo acceso a la información relacionada con los **Sistema de la Municipalidad**: _____ (nombre del sistema o el tipo de cuenta)

Entiendo que toda la información no publica tiene el carácter de confidencialidad, está sujeta a reserva por mi parte y solo puedo utilizar la información para los fines que mis responsabilidades como empleado de la Municipalidad de Villa El Salvador requiera.

Entiendo que, en algunos casos, la publicación, traspaso no autorizado o mal uso de información confidencial puede ser sancionado.

Me comprometo a:

1. No divulgar información confidencial, por ningún medio, sin un permiso escrito de la Municipalidad de Villa El Salvador
2. Proteger la información confidencial de ser divulgada o mal utilizada.
3. Usar la información confidencial solo para uso estricto en las funciones que como empleado realizo en Municipalidad de Villa El Salvador.
4. Devolver a la Municipalidad de Villa El Salvador cualquier información confidencial que pueda tener en mi poder cuando termine mi trabajo, o antes si la Municipalidad así me lo solicita.

RECOMENDACIONES PARA LA MANIPULACION Y ALMACENAMIENTO DE INFORMACION

Las Recomendaciones que se establecen en este anexo es con el objeto de proteger la información que manejan los usuarios de los diversos sistemas de la Municipalidad de Villa El Salvador. Por ello, los usuarios deben proceder con un criterio de prudencia que, en muchos casos y dependiente de las circunstancias, implica adoptar resguardos superiores a aquellos aquí consignados. Las siguientes recomendaciones constituyen un mínimo a aplicar y debe ser acatadas por los empleados a quienes se asigna un usuario al **Sistema de la Municipalidad**: _____ (nombre del sistema o tipo de Cuenta)

1. Nunca Compartir Claves.
2. Cambiar las Claves al menos cada 2 meses procurando que ellos cumplan estándares de seguridad.
3. No acceder a copias de información o bases de datos confidenciales a los cuales no se tiene acceso autorizado.
4. No generar copias totales o parciales de información que puedan circular o manipularse sin el nivel requerido de resguardo o facilitar su uso por personas no autorizadas.
5. Evitar trasladar información confidencial fuera de la oficina y por motivos distintos a realizar labores de trabajo (reuniones o trabajo extraordinario y justificado)

Firma:

DNI: _____

Fecha: _____

Unidad de Desarrollo Tecnológico





11.2. Anexo 2: Reestablecer Contraseña

	MUNICIPALIDAD DISTRITAL DE VILLA EL SALVADOR	FORMULARIO Nro. 3 REESTABLECER CONTRASEÑA	VERSIÓN: 4.0 PAGINA: 1 de 1
--	--	--	--------------------------------

(Debe ser llenado por el Usuario y con letra imprenta)

Referencia al Memorando Nro.					
Fecha de la Solicitud:	/	/	(dd/mm/aaaa)		
TIPO DE CUENTA A REESTABLECER CONTRASEÑA (marcar solo una opción)					
Marcar con X	Sistema Informático		Correo Institucional	Usuario PC (red munives)	VPN usuario (CAS/Fijo)
	<i>Si marca Sistema Informático, llenar: (marcar una opción)</i>			<i>Si marca Usuario PC o VPN, llenar:</i>	
	<input type="checkbox"/> SIGAMEF	<input type="checkbox"/> SITRADO (actual)	<input type="checkbox"/> RENTAS GISMUN	Cod. Patrimonial CPU:	
	<input type="checkbox"/> RUOS	<input type="checkbox"/> SIAF MVES	<input type="checkbox"/> SIAF Mancomunidad		
	<input type="checkbox"/> RENTAS (antigua)	<input type="checkbox"/> SIGAVES (antigua)	<input type="checkbox"/> SISCOMP. (Sist. Comprob.)		
<input type="checkbox"/> SIGAVES	<input type="checkbox"/> OTROS				
Especificar (si marco otros):					
DATOS DEL USUARIO					
Cuenta o Usuario (login):		DNI o Pasaporte:			
Nombres y Apellidos:					
Motivo:		Régimen Laboral:			
Sede:		Unidad Orgánica:			
Jefe Inmediato:					

TÉRMINOS DE RESPONSABILIDADES:

- **El responsable de la Unidad Orgánica:** Es el único autorizado a solicitar la recuperación de contraseña de las cuentas de usuarios. Estará obligado a comunicar a la Unidad de Desarrollo Tecnológico (UDT), siempre que se sucedan cambios en las cuentas de los usuarios habilitados.
- **El usuario será el único responsable:** Responsable en el manejo que se le dé a la información a la que tiene acceso. Atender y aplicar el acuerdo de Confidencialidad y las Recomendaciones para la Manipulación y Almacenamiento de Información que se mencionan a continuación se le enviara con la relación permisos asignados, si no está de acuerdo con algún o algunos de los términos definidos por favor solicite la desactivación de su usuario.

Firma y sello Jefe Inmediato

Firma del Usuario.

Unidad de Desarrollo Tecnológico





11.3. Anexo3: Formulario Préstamo de Equipo Informático

	MUNICIPALIDAD DISTRITAL DE VILLA EL SALVADOR	FORMULARIO Nro. 05	VERSIÓN: 2.0
		PRESTAMO DE EQUIPOS INFORMATICOS Y/O DISPOSITIVOS	PÁGINA: 1 de 1

(Debe ser llenado por el Usuario y con letra imprenta)

Nro. Solicitud: (nro.-area-año)			
Fecha de la Solicitud: / / (dd/mm/aaaa)			
Cantidad ítem:			
EQUIPOS INFORMATICOS O DISPOSITIVOS			
Solicito:	<input type="checkbox"/> CPU	<input type="checkbox"/> Monitor	<input type="checkbox"/> Laptop
(en el recuadro colocar cantidad)	<input type="checkbox"/> Proyector	<input type="checkbox"/> Estabilizador	<input type="checkbox"/> Teclado
	<input type="checkbox"/> Impresora / Multifuncional	<input type="checkbox"/> Mouse	
	<input type="checkbox"/> Otros		
DATOS DEL AREA SOLICITANTE			
Sede:			
Unidad Orgánica:			
Jefe Inmediato:			
Usuario Solicitante:			
DNI u Otro Doc. de Identidad:			
Teléf. o anexo:		Correo:	
Periodo de préstamo:			
Motivo:			

El Área deberá responder por cualquier daño o perdida parcial o total, será responsabilidad devolver el equipo de cómputo o dispositivo en buenas condiciones dentro del periodo establecido de servicio.

Al Firmar entiendo y acepto los términos y las condiciones mencionadas anteriormente.

Firma de Conformidad

Firma y sello del Jefe Inmediato

Firma del Usuario Solicitante



Unidad de Desarrollo Tecnológico



MUNICIPALIDAD
DISTRITAL DE
VILLA EL
SALVADOR

FORMULARIO Nro. 06
ENTREGA DE EQUIPOS INFORMATICOS EN
CALIDAD DE PRESTAMO

VERSIÓN: 2.0

PÁGINA: 2 de 2

Subgerente UDT
DEVOLUCION DE EQUIPOS INFORMATICO EN ESTADO DE PRESTAMO
(Anexo1)

(Debe ser llenado por el Técnico y con letra imprenta)

Nro. Referencial de la solicitud.

Fecha de Devolución: / / (dd/mm/aaaa)

DATOS DE LOS EQUIPOS INFORMATICOS Y/O DISPOSITIVOS

Tipo de Equipo	Código Patrimonial	Marca	Modelo	Serie	Mac

REVISION DEL EQUIPO INFORMATICO Y/O DISPOSITIVO

Técnico Responsable:

Inspeccionado:	<input type="checkbox"/>	SI	<input type="checkbox"/>	NO
Daños Visibles:	<input type="checkbox"/>	SI	<input type="checkbox"/>	NO
Estado:	<input type="checkbox"/>	Operativo	<input type="checkbox"/>	Inoperativo

Observación:

Jefe Inmediato:

Usuario Responsable:

El Usuario será responsable de guardar o realizar copias de todos los documentos y otros trabajos que haya realizado.

Firma de Conformidad

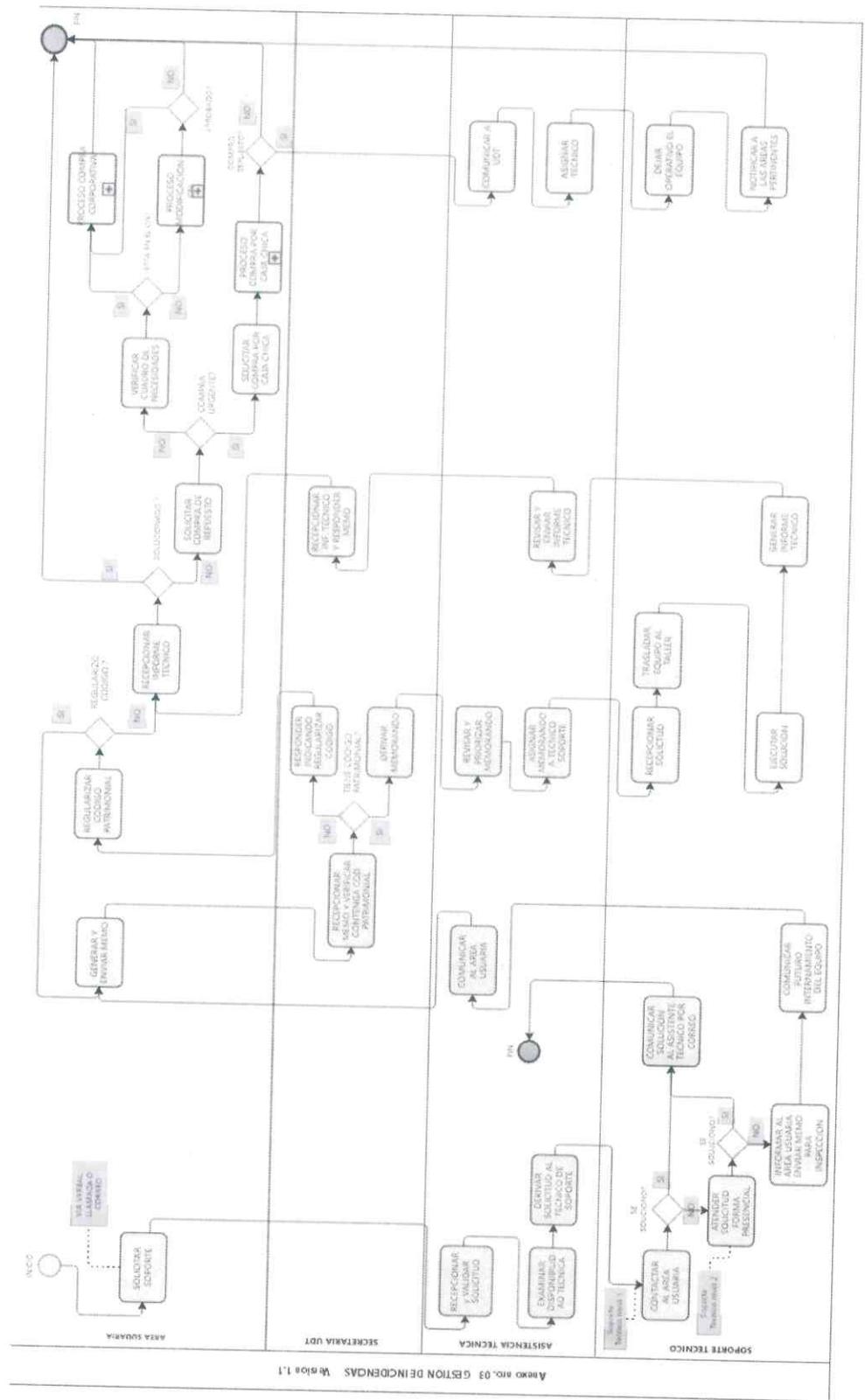
Firma del Usuario Responsable
(quien devuelve equipo informático)

Firma del Técnico Responsable
(quien recibe equipo informático)





11.5. Anexo 5: Diagrama de Flujo : Mesa de Ayuda - Soporte Técnico



Anexo Nro.04 : “Procesos de Backup’s de Base de Datos de Sistemas e Información General de la Municipalidad Distrital de Villa El Salvador”

Software que realiza proceso de BACKUP:

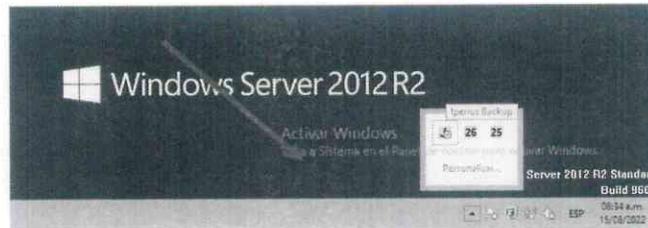
IMPERIUS BACKUP (No Licenciado)



Características del Servidor donde se realizan las y FILE SERVER:

configuraciones para los backups de BD

Procesador : Intel (R) Dual CPU E2160 @1.80 GHZ
 Memoria RAM : 6.00 GB
 Discos Duros : C:\ (sistema operativo - 150GB)
 D:\ (almacén de datos – 5TB)



Listado de BACKUPS realizados diariamente

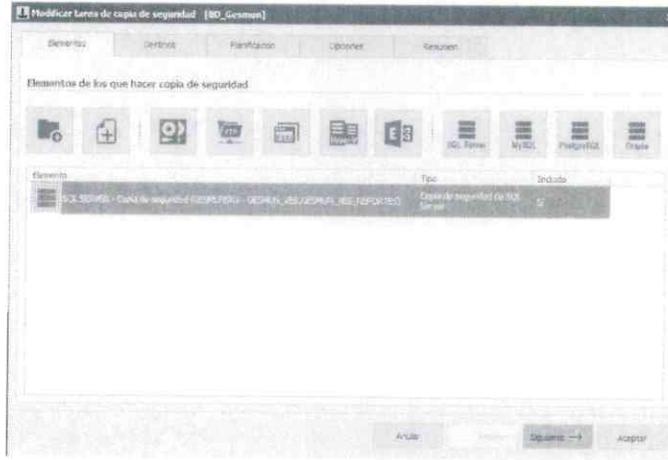
Tarea de copia de seguridad	Última ejecución	Último resultado	Estado / Información sobre la última copia de seguridad
BD_Gesmun	04/08/2022 11:01:53 p.m.	Copia de seguridad completada correctamente	164,7 GB - 4 archivos (01:22:20)
BD_Ruos	12/08/2022 08:00:02 p.m.	Copia de seguridad completada correctamente	11,7 MB - 71 archivos (00:00:18)
BD_Siaf_Completo	01/08/2022 11:02:09 p.m.	Copia de seguridad completada correctamente	37,9 GB - 26753 archivos (02:26:49)
BD_Siaf_Mancomunidad	12/08/2022 10:00:22 p.m.	Copia de seguridad completada correctamente	652,4 MB - 2599 archivos (00:03:51)
BD_Siaf	15/08/2022 01:00:25 a.m. (Hoy)	Copia de seguridad completada correctamente	8,0 GB - 2761 archivos (00:26:13)
BD_SigaMEF	04/08/2022 11:00:23 p.m.	Copia de seguridad completada correctamente	3,0 GB - 2 archivos (00:01:28)
BD_Sistradoc	12/08/2022 08:00:22 p.m.	Copia de seguridad completada correctamente	169,1 MB - 57 archivos (00:01:04)
BD_Sitradoc	12/08/2022 10:00:00 p.m.	Copia de seguridad completada correctamente	313,0 MB - 2 archivos (00:00:21)
BD_Zincron	15/08/2022 03:00:42 a.m. (Hoy)	Copia de seguridad completada correctamente	2,3 GB - 191 archivos (00:06:46)
CENTROS DE COSTO	12/08/2022 10:04:16 p.m.	Copia de seguridad completada correctamente	38,9 GB - 97226 archivos (48:03:34)



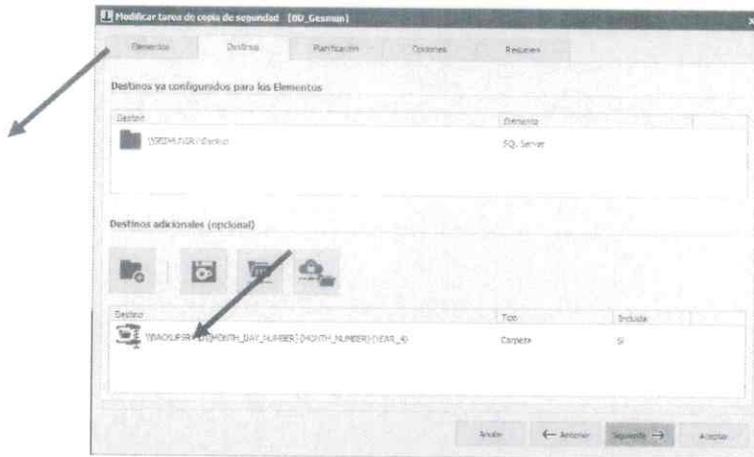


Proceso:

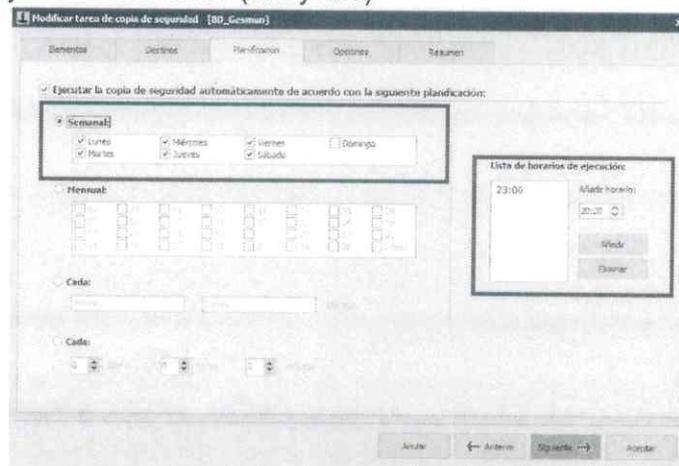
- Indica la BD que cargará (origen)



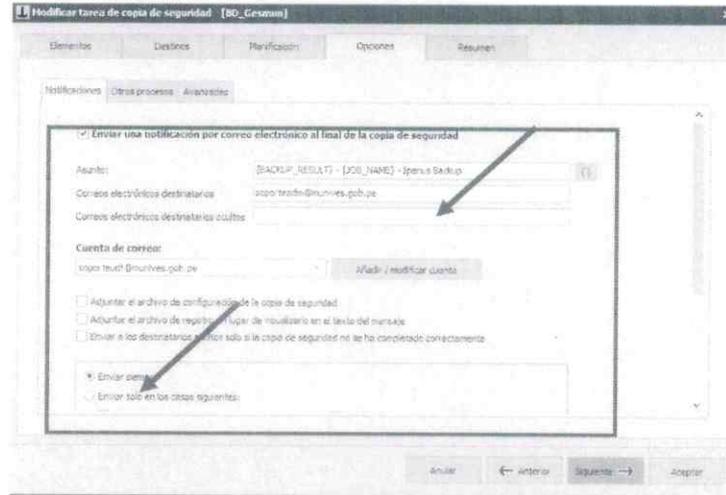
- Destino (ubicación) de respaldo del BACKUP de la BD al primer respaldo en la ubicación \\GEMUNSRV\Backup y el método de compresión a la segunda ubicación \\BACKUPSRVD



- Programación de la ejecución de BACKUP (días y hora)



- Notificación permanente al correo para la validación del proceso

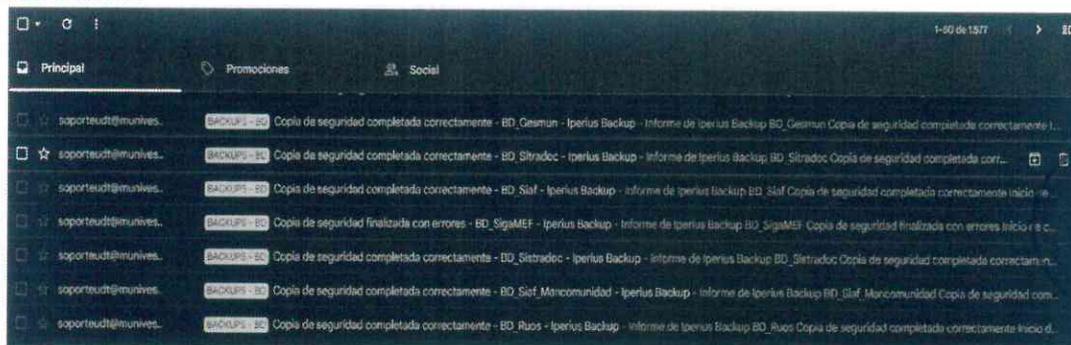


- El procedimiento se realizará para cada uno de los registros



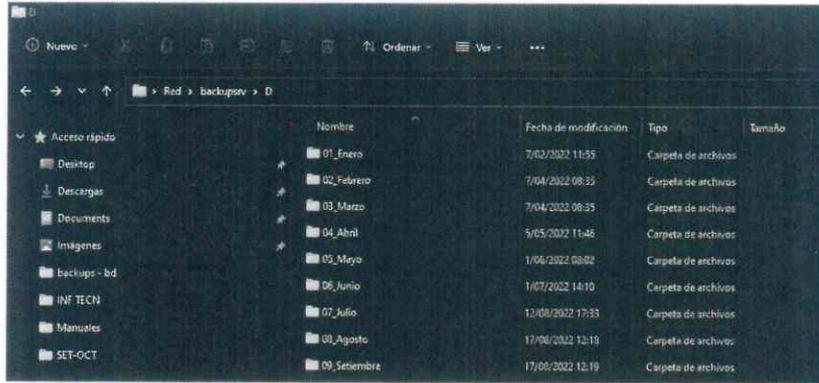
Al finalizar el proceso se validará con el correo remitido y las BD copiadas en la ubicación \\BACKUPSRVD

Correo recibido:

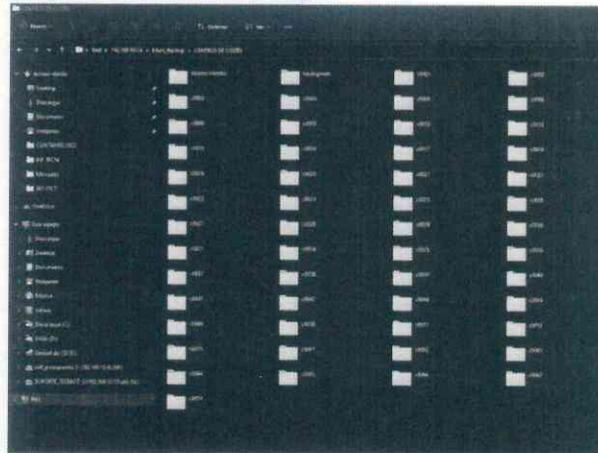


Confirmación de archivos guardados

\\BACKUPSRVD



\\192.168.10.14\Muni_Backup\CENTROS DE COSTO



- Al mismo tiempo se ha creado una bitácora en línea de los backups de BD para su validación por cada responsable del sistema y control diario de los procesos

Link:

https://docs.google.com/spreadsheets/d/1_r89IFqgVN4gqLbdScW2R5auIvctjmEMCGX47aC4rHE/edit#gid=0

BITACORA DE COPIA DE SEGURIDAD

ITEM	FECHA BACKUP	SERVIDOR ORIGEN (IP)	SERVIDOR DESTINO (IP)	NOMBRE DE TAREA BACKUP	TIPO DATO (.DBF, .ZIP)	NRO. ARCH.	TAMAÑO	ESTADO (validación)	RESPONSABLE (CARGO)	EVIDENCIA
1	01-08-2022	PHYSERV	1192.168.10.2346	BD_Runa	BD_Runa_01082022_2300001.zip	1	2.885 KB		Coordinador de Soporte	https://docs.google.com/spreadsheets/d/1_r89IFqgVN4gqLbdScW2R5auIvctjmEMCGX47aC4rHE/edit#gid=0
2	02-08-2022	SIAPSERV	1192.168.10.2346	BD_SiA	BD_SiA_02082022_2300001.zip	1	1.507.248 KB		Coordinador de Soporte	https://docs.google.com/spreadsheets/d/1_r89IFqgVN4gqLbdScW2R5auIvctjmEMCGX47aC4rHE/edit#gid=0
3	03-08-2022	SIAPSERV	1192.168.10.2346	BD_SiA_Completo	BD_SiA_Completo_03082022_2300001.zip	1	10.348.736 KB		Coordinador de Soporte	https://docs.google.com/spreadsheets/d/1_r89IFqgVN4gqLbdScW2R5auIvctjmEMCGX47aC4rHE/edit#gid=0
4	04-08-2022	SIAPSERV	1192.168.10.2346	BD_SiA_Mantenimiento	BD_SiA_Mantenimiento_04082022_2300001.zip	1	9.663 KB		Coordinador de Soporte	https://docs.google.com/spreadsheets/d/1_r89IFqgVN4gqLbdScW2R5auIvctjmEMCGX47aC4rHE/edit#gid=0
5	05-08-2022	SIAPSERV	1192.168.10.2346	BD_Sigafit	BD_Sigafit_05082022_2300001.zip	1	392.746 KB		Coordinador de Soporte	https://docs.google.com/spreadsheets/d/1_r89IFqgVN4gqLbdScW2R5auIvctjmEMCGX47aC4rHE/edit#gid=0
6	06-08-2022	PHYSERV	1192.168.10.2346	BD_Sistema	BD_Sistema_06082022_2300001.zip	1	41.404 KB		Coordinador de Soporte	https://docs.google.com/spreadsheets/d/1_r89IFqgVN4gqLbdScW2R5auIvctjmEMCGX47aC4rHE/edit#gid=0
7	07-08-2022	SIAPSERV	1192.168.10.2346	BD_Sistema	BD_Sistema_07082022_2300001.zip	1	70.243 KB		Coordinador de Soporte	https://docs.google.com/spreadsheets/d/1_r89IFqgVN4gqLbdScW2R5auIvctjmEMCGX47aC4rHE/edit#gid=0
8	08-08-2022	PHYSERV	1192.168.10.2346	BD_Sistema	BD_Sistema_08082022_2300001.zip	1	178.372 KB		Coordinador de Soporte	https://docs.google.com/spreadsheets/d/1_r89IFqgVN4gqLbdScW2R5auIvctjmEMCGX47aC4rHE/edit#gid=0
9	09-08-2022	SIAPSERV	1192.168.10.2346	BD_Sistema	BD_Sistema_09082022_2300001.zip	1	20.989.729 KB		Coordinador de Soporte	https://docs.google.com/spreadsheets/d/1_r89IFqgVN4gqLbdScW2R5auIvctjmEMCGX47aC4rHE/edit#gid=0
10	10-08-2022	PHYSERV	1192.168.10.2346	BD_Runa	BD_Runa_10082022_2300001.zip	1	2.883 KB		Coordinador de Soporte	https://docs.google.com/spreadsheets/d/1_r89IFqgVN4gqLbdScW2R5auIvctjmEMCGX47aC4rHE/edit#gid=0
11	11-08-2022	SIAPSERV	1192.168.10.2346	BD_SiA_Mantenimiento	BD_SiA_Mantenimiento_11082022_2300001.zip	1	9.663 KB		Coordinador de Soporte	https://docs.google.com/spreadsheets/d/1_r89IFqgVN4gqLbdScW2R5auIvctjmEMCGX47aC4rHE/edit#gid=0
12	12-08-2022	SIAPSERV	1192.168.10.2346	BD_Sigafit	BD_Sigafit_12082022_2300001.zip	1	392.746 KB		Coordinador de Soporte	https://docs.google.com/spreadsheets/d/1_r89IFqgVN4gqLbdScW2R5auIvctjmEMCGX47aC4rHE/edit#gid=0
13	13-08-2022	PHYSERV	1192.168.10.2346	BD_Sistema	BD_Sistema_13082022_2300001.zip	1	41.404 KB		Coordinador de Soporte	https://docs.google.com/spreadsheets/d/1_r89IFqgVN4gqLbdScW2R5auIvctjmEMCGX47aC4rHE/edit#gid=0
14	14-08-2022	SIAPSERV	1192.168.10.2346	BD_Sistema	BD_Sistema_14082022_2300001.zip	1	70.243 KB		Coordinador de Soporte	https://docs.google.com/spreadsheets/d/1_r89IFqgVN4gqLbdScW2R5auIvctjmEMCGX47aC4rHE/edit#gid=0
15	15-08-2022	PHYSERV	1192.168.10.2346	BD_Sistema	BD_Sistema_15082022_2300001.zip	1	178.372 KB		Coordinador de Soporte	https://docs.google.com/spreadsheets/d/1_r89IFqgVN4gqLbdScW2R5auIvctjmEMCGX47aC4rHE/edit#gid=0



	MUNICIPALIDAD DE VILLA EL SALVADOR	Año: 2022
	POLITICAS DE SEGURIDAD DE LA INFORMACION	Versión: 1.0
		Página: 48 de 72

Anexo Nro.05 : “Implementación de Directorio Activo y Administrativo de Usuarios en la Municipalidad Distrital de Villa El Salvador”

1. Objetivo

Contar con un procedimiento para la Administración de los Usuarios del servicio de Directorio Activo de la Municipalidad de Villa El Salvador a cargo del personal asignado a Soporte Técnico, Redes y Telecomunicaciones de la UDT.

2. Alcance

El alcance de este procedimiento está orientado al personal responsable del Soporte Técnico, Redes y Telecomunicaciones de la UDT

3. Definiciones.

- **Hardware:** Conjunto de componentes materiales o físicos de un sistema informático, cada una de las partes que conforman un computador, incluidos sus periféricos.
- **Software:** Es un conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en un computador, se considera que el software es el equipamiento lógico e intangible de un computador.
- **Computador:** Es una maquina electrónica cuya principal función es la de procesar grandes cantidades de información en forma veloz y precisa, y que realiza este procedimiento gracias al hardware y software.
- **Red Informática:** Es un conjunto de dispositivos y equipos de cómputo como computadores y servidores que esta interconectados entre si sobre un medio físico, que intercambian información y comparten recursos.
- **Servidor:** Computador que forma parte de una red informática y que provee determinados servicios al resto de los computadores de la misma red, llamados a su vez estaciones o clientes. Dicho computador debe contar con una aplicación específica capaz de atender las peticiones de los distintos clientes y brindarles respuesta oportuna, por lo tanto, dentro de este computador físico (Hardware) pueden funcionar varios servidores simultáneos, siempre y cuando cuenten con los recursos necesarios para ello.
- **Servidor de Directorio Activo / Dominio:** Servidor encargado de Administrar la información relacionada con la red informática, sus usuarios, equipos y grupos internos.
- **Aplicación:** Es un programa informático diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de tareas, esto lo diferencia principalmente de otros tipos de programas, las aplicaciones pertenecen a la categoría de software de aplicación.
- **Servicio de directorio:** Es una aplicación o conjunto de aplicaciones que almacena y organiza la información sobre los usuarios de una red de computadores y sobre los recursos de red que permite a los administradores gestionar el acceso de los usuarios a los recursos sobre dicha red.
- **Active Directory / Directorio Activo (AD):** Es un servicio de directorio desarrollado por la empresa Microsoft, para su uso en entornos Windows Server, establecido en uno o varios servidores en donde se crean objetos tales como usuarios, equipos o grupos, con el objetivo de administrar los inicios de sesión en los equipos conectados a la red, así como también las políticas en toda la red, utiliza distintos protocolos de aplicación y autenticación como: LDAP, DNS, DHCP y Kerberos.
- **Dominio de Active Directory:** Unidad administrativa principal de un Directorio Activo (AD) alberga en él, diversos objetos tales como: usuarios, equipos, relaciones de confianza, autenticación, Administración de directivas de grupo (GPO), Replicación.
- **Controlador de Dominio:** Los controladores de dominio son servidores de Windows que contienen la base de datos de Active Directory y ejecutan funciones relacionadas con Active Directory, como la autenticación, que es proceso otorgar o denegar a un usuario el acceso a recursos compartidos o a otra máquina de la red, normalmente a través del uso de una contraseña.



	MUNICIPALIDAD DE VILLA EL SALVADOR	Año: 2022
	POLITICAS DE SEGURIDAD DE LA INFORMACION	Versión: 1.0
		Página: 49 de 72

- **Equipos de Dominio:** Equipos de cómputo que se encuentran administrados por los servicios de Active Directory.
- **Usuario de Dominio:** Cuenta de usuario del dominio a la cual se le puede asignar derechos, permisos y restricciones de acceso dentro de la red del dominio.
- **UDT:** Unidad de Desarrollo Tecnológico, es un órgano de apoyo, encargado de gestionar los recursos TI de la Municipalidad Distrital de Villa El Salvador.
- **MVES :** Municipalidad Distrital de Villa El Salvador, es la institución del estado con personería jurídica, facultada para ejercer el gobierno de un distrito o provincia.

4. Marco Legal

1. DL. N° 604, Ley de Organización y Funciones del INEI.
2. DS. N° 018-91-PMC, Reglamento de Organización y Funciones del INEI.
3. RJ. N° 340-94-INEI, Normas Técnicas para el procesamiento y respaldo de la información que se procesa en entidades del Estado.
4. RJ. N° 076-95-INEI, Recomendaciones Técnicas para la seguridad e integridad de la información que se procesa en la administración pública.
5. RJ. N° 090-95-INEI, Recomendaciones Técnicas para la protección física de los equipos y medios de procesamiento de la información en la administración pública.
6. Ley orgánica de Municipalidades N° 27972 Artículo 20° inciso 6) del 27-05-2003 (Dictar decretos y resoluciones de alcaldía, con sujeción a las leyes y ordenanzas).
7. Ordenanza N° 298 del 29 de abril del 2014, que aprueba el Nuevo Reglamento de Organización y Funciones de La Municipalidad de Villa El Salvador.
8. Decreto de alcaldía 025-2008-ALC/MVES DEL 31 de agosto de 2008 sobre "Uso de equipos informáticos, red, internet y correo electrónico".

5. Responsabilidad y Autoridad

La responsabilidad de elaborar el presente manual la tiene la UDT y Estadística a través el área de soporte técnico, redes y telecomunicaciones.



6. Estado situacional de la implementación del directorio activo de la Municipalidad de Villa El Salvador:

6.1 Implementación Del Dominio Active Directory Munives

6.1.1 Justificación de la Implementación

La implementación del dominio Active Directory "MVES" surge de la necesidad de la municipalidad Distrital de Villa El Salvador de tener una solución que le permita una administración centralizada de los equipos informáticos, el uso eficiente de los recursos y la seguridad de la red informática municipal.

6.1.2 Implementación Del Dominio De Red

Se cambió la forma de administración de la red informática municipal, pasando de un esquema de grupos de trabajo independientes, a una red informática municipal administrada y centralizada a través de Active Directory, con esto se centralizará el control de los usuarios y recursos, optimizando las labores de administración, desde el punto de vista de la seguridad, la implementación del dominio permite tener un mayor control en el acceso a los equipos y la información, mejorando los servicios de seguridad como la autenticación y el control de acceso mediante el uso de contraseñas que todos los usuarios del dominio tienen, para que los usuarios puedan iniciar sesión en un equipo de cómputo que pertenezca al dominio de la red informática municipal, se requieren credenciales de identificación de los usuarios, es decir, nombre de usuario y contraseña.



6.1.3 Arquitectura Del Dominio Active Directory

Tabla: Especificaciones técnicas del Servidor de Active Directory:

La implementación de Active Directory se encuentra alojada en un servidor virtualizado del tipo Microsoft Hyper-V, del mismo modo este servidor virtualizado se encuentra alojado en un servidor físico con las siguientes características principales:

SERVIDOR FISICO					
MARCA	MODELO	PROCESADOR	RAM	DISCO DURO	SISTEMA OPERATIVO
HP	Proliant DL380 Gen10	Intel Xeon E5-2630 v3 2.40 Ghz /16 CPUs)	98 GB	5 TB	Windows Server 2016 DC

Características del Servidor Virtualizado:

SERVIDOR VIRTUALIZADO				
SOFTWARE DE VIRTUALIZACION	Nº NUCLEOS	RAM	DISCO VIRTUAL	SISTEMA OPERATIVO
Microsoft Hyper-V	4	4 GB	160 GB	Windows Server 2016 Standar

6.1.4 Requisitos Para La Administración De Usuarios Del Dominio:

Para poder comenzar a administrar el servicio de Active Directory se debe seguir con los siguientes pasos:

- Un servidor con Windows Server instalado, en la presente implementación se utilizó la versión Windows Server 2016, con el rol de servicios de Dominio de Active Directory correctamente instalado y configurado.
- Las herramientas de administración se pueden ejecutar desde el servidor, pero también es posible ejecutar las herramientas desde una consola remota.
- Para realizar los procedimientos que se incluyen en este documento será necesario haber iniciado sesión como usuario con privilegios administrativos en el servidor.

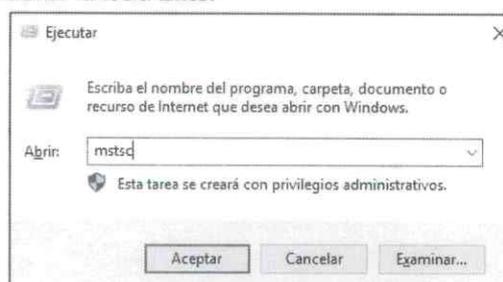


6.1.5 Pasos Para El Acceso Al Complemento Usuarios Y Equipos De Active Directory En El Servidor De Dominio.

Para iniciar la Administración de Usuarios del servicio de directorio Active Directory se deberá seguir con los siguientes pasos:

Pasos:

1. Presionar las teclas  + , se mostrará la ventana "Ejecutar", y escribir en el cuadro de texto "Abrir": **mstsc** y luego presionar la tecla **Enter**



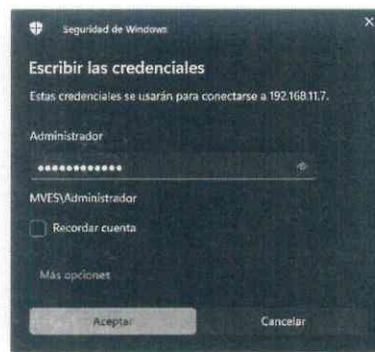
Como resultado de esta acción se mostrará la siguiente ventana, en el cuadro **“Equipo”** se deberá escribir la dirección del servidor:

- IP del Controlador de Dominio Principal: **192.168.11.7**

Luego hacer clic en **“Conectar”**.



Luego se mostrará una ventana donde deberá autenticarse con un usuario con privilegios de **Administración del Dominio**, luego hacer clic en **Aceptar**

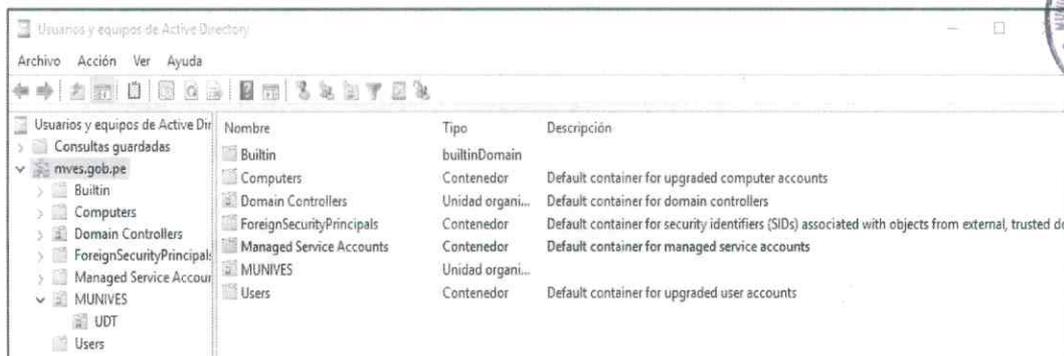


Una vez que ingresemos al servidor deberemos buscar en el escritorio el siguiente icono **“Usuarios y equipos de Active Directory”**:

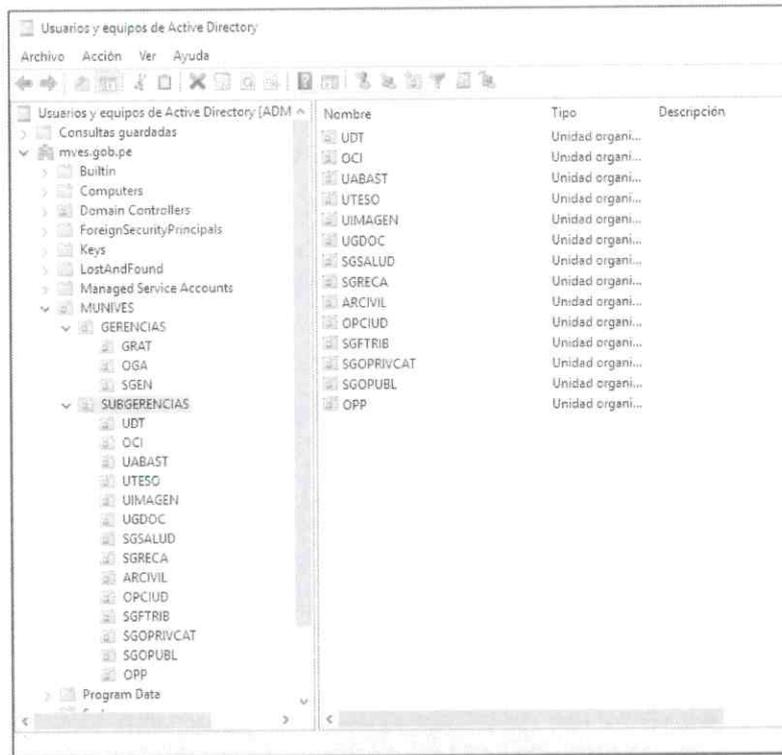


Luego hacemos doble clic sobre él.

Como resultado de esta acción se nos mostrara la consola **“Usuarios y equipos de Active Directory”**



- Se debe expandir **ad.mves.gob.pe** haciendo clic en el símbolo (>) para visualizar la estructura organizacional de nuestro directorio activo, el mismo que ya cuenta con unidades organizativas, grupos y usuarios.
- Hasta el momento se han creado las siguientes unidades organizativas dentro del dominio con el fin tener organizados a los usuarios de dominio:



UNIDAD ORGANIZATIVA	DESCRIPCION
MUNIVES	Unidad Organizativa que contiene a todas las Gerencias y Subgerencias de la Organización y todos los usuarios del dominio.
Gerencias	Unidad Organizativa que contiene a las Gerencias de la Municipalidad
GRAT	Unidad Organizativa que contiene a los usuarios de la Gerencia de Rentas y Administración Tributaria
OGA	Unidad Organizativa que contiene a los usuarios de la Oficina General de Administración
SGEN	Unidad Organizativa que contiene a los usuarios de la Secretaria General
Subgerencias	Unidad Organizativa que contiene a las Subgerencias de la Municipalidad
UDT	Unidad Organizativa que contiene a los usuarios de la Unidad de Desarrollo Tecnológico
OCI	Unidad Organizativa que contiene a los usuarios de la Oficina de Control Interno



	MUNICIPALIDAD DE VILLA EL SALVADOR	Año: 2022
	POLITICAS DE SEGURIDAD DE LA INFORMACION	Versión: 1.0
		Página: 53 de 72

UABAST	Unidad Organizativa que contiene a los usuarios de la Unidad de Abastecimiento
UTESO	Unidad Organizativa que contiene a los usuarios de la Unidad de Tesorería
UIMAGEN	Unidad Organizativa que contiene a los usuarios de la Unidad de Imagen Institucional
UGDOC	Unidad Organizativa que contiene a los usuarios de la Unidad de Gestión Documentaria
SGSALUD	Unidad Organizativa que contiene a los usuarios de la Subgerencia de Salud, Sanidad y Bienestar Social
SGRECA	Unidad Organizativa que contiene a los usuarios de la Subgerencia de Recaudación y Control
ARCIVIL	Unidad Organizativa que contiene a los usuarios de la Subgerencia de Registro Civil y Cementerio
OPCIUD	Unidad Organizativa que contiene a los usuarios de la Subgerencia de Participación Ciudadana
SGFTRIB	Unidad Organizativa que contiene a los usuarios de la Subgerencia de Fiscalización Tributaria
SGOPCAT	Unidad Organizativa que contiene a los usuarios de la Subgerencia de Obras Privadas y Catastro
SGOPUBL	Unidad Organizativa que contiene a los usuarios de la Subgerencia de Obras Públicas
OPP	Unidad Organizativa que contiene a los usuarios de la Oficina de Presupuesto y Planificación
SGFADM	Unidad Organizativa que contiene a los usuarios de la Subgerencia de Fiscalización Administrativa
SGSEREN	Unidad Organizativa que contiene a los usuarios de la Subgerencia de Serenazgo

4. Los objetos que se describen en la siguiente tabla se crean automáticamente durante la instalación del rol de Active Directory en el servidor:

Icono	Carpeta	Descripción
	Dominio	Este objeto representa nodo raíz del dominio administrado en nuestro caso el dominio ad.mves.gob.pe .
	Builtin	Este objeto contiene información de grupos administrativos que se han creado de forma automática en el contenedor.
	Computers	Contiene todos los equipos Windows 7, Windows 8, Windows 10 y Windows 11 que han sido agregados al dominio.
	Users	Contiene los grupos administrativos que se han creado de forma automática en el contenedor Usuarios.



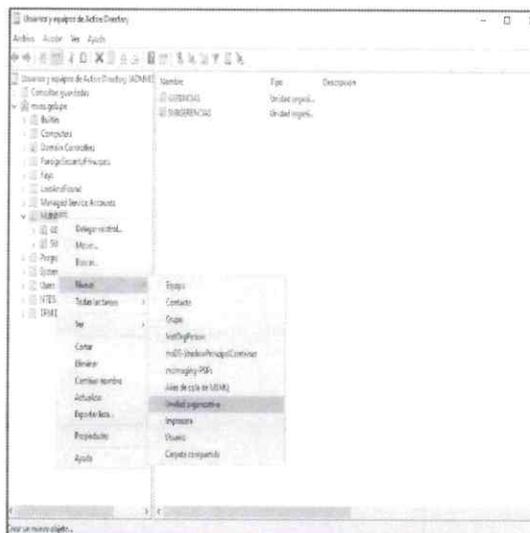
Se puede usar Active Directory para crear los siguientes objetos:

Icono	Objeto	Descripción
	Usuario	Un objeto Usuario es una entidad de seguridad en el directorio. Un usuario puede iniciar una sesión en la red con sus respectivas credenciales y a los usuarios se les puede conceder permisos de acceso
	Contacto	Un objeto Contacto es una cuenta que no tiene ningún permiso de seguridad. No se puede iniciar sesión como contacto. Los contactos se usan con frecuencia para representar a usuarios externos asociados con el correo electrónico.
	Equipo	Es un objeto que representa a un equipo en la red, para las estaciones de trabajo y servidores Windows, esta es la cuenta de equipo.
	Unidad Organizativa	Las Unidades Organizativas se utilizan como contenedores para organizar de manera lógica objetos de directorio como son los: Usuarios, Grupos y Equipos, de forma similar a como se utilizan las carpetas para organizar archivos en las unidades de almacenamiento.
	Grupo	Los Grupos pueden contener Usuarios, Equipos y otros Grupos, los grupos simplifican la administración de cantidades grandes de objetos.
	Carpeta compartida	Una carpeta compartida es un recurso compartido de red que se ha publicado en el directorio
	Impresora compartida	Una impresora compartida es una impresora de red que se ha publicado en el directorio

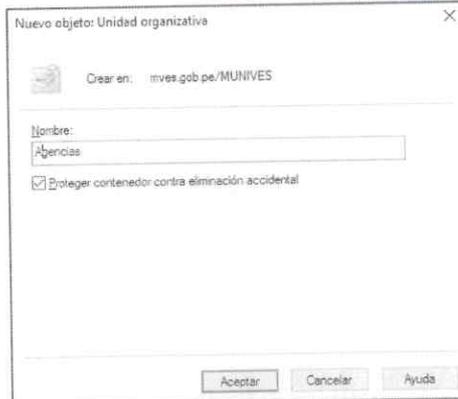
6.1.6 Pasos Para La Creación De Unidades Organizativas Y Usuarios En El Dominio

Crear una nueva Unidad Organizativa dentro del dominio:

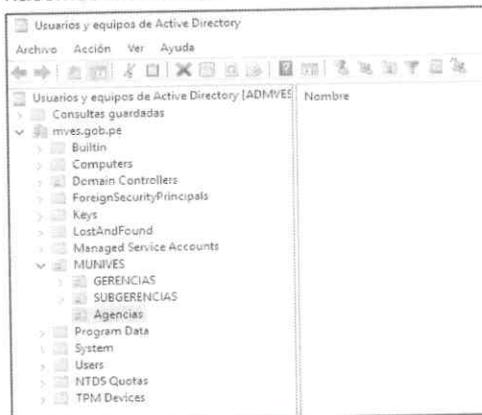
1. Se deberá hacer clic con el botón secundario del mouse sobre el objeto del dominio donde se desee crear una nueva Unidad Organizativa.



2. En el menú se deberá seleccionar la opción “Nuevo”, y luego hacer clic en “Unidad organizativa”



3. En la ventana que nos aparecerá se deberá escribir el nombre respectivo de acuerdo a la estructura de la organización, luego hacemos clic en OK.



Finalmente validamos en la consola que nuestra Unidad Organizativa se haya creado en el lugar que seleccionamos en la estructura del dominio.

Crear un nuevo usuario de dominio:

Antes de proceder a crear una nueva cuenta de usuario se debe tomar en cuenta lo siguiente:

- El nombre de la cuenta a crear debe identificar ya sea el nombre real del usuario o el uso que se le va a dar a la cuenta.
- **La Unidad Organizativa** donde se va a crear el usuario
- Los nombres asignados a los usuarios deben ser únicos, si existe un gran número de usuarios, la asignación de nombres debe contar con la posibilidad de empleados con nombres iguales, en estos casos se determinará un criterio a seguir para no asignar el mismo nombre de usuario a dichos usuarios.

Por ejemplo: Oscar Palacios podría tener las siguientes cuentas: Jguizado, Jguizadoc, Guizadoc o Joguic, etc.

En el caso de la implementación se utilizó el formato de la inicial del primer nombre seguido del apellido paterno, por ejemplo:

José Guizado Castillo	→	jguizado
Deborah Fuentes Flores	→	dflores
Macpierre Carbonero Condezo	→	mcarbonero

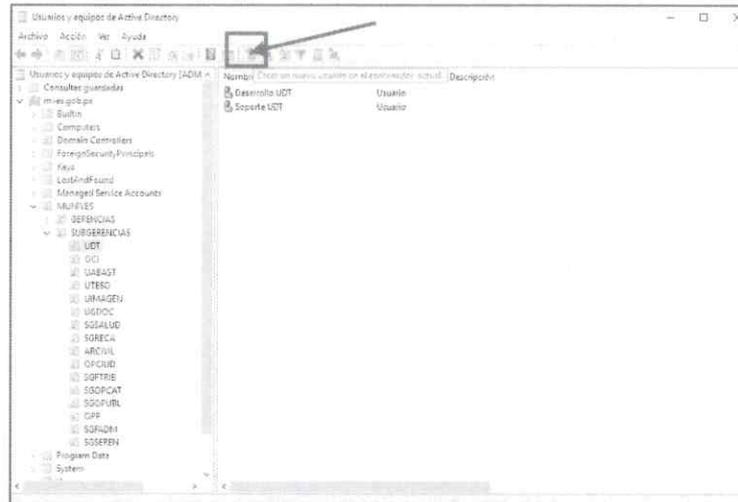


	MUNICIPALIDAD DE VILLA EL SALVADOR	Año: 2022
	POLITICAS DE SEGURIDAD DE LA INFORMACION	Versión: 1.0
		Página: 56 de 72

En caso existieran usuarios con el nombre igual se utilizará la inicial del apellido materno, dando prioridad al primer usuario creado, por ejemplo:

José Guizado Castillo → **jguizado**
 Juan Guizado Morales → **jguizadom**

1. Para crear un nuevo usuario se deberá hacer clic con el botón primario del mouse sobre la Unidad Organizativa en la cual se agregará la nueva cuenta de usuario, hacer clic en el botón “nuevo usuario” de la barra de herramientas.



2. Luego en esta ventana se deberán rellenar los siguientes campos:

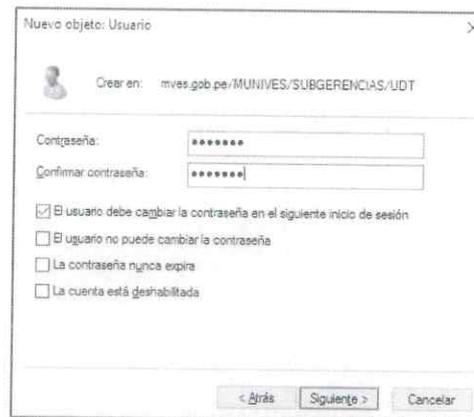
- **Nombre de pila:** Nombres del usuario
- **Iniciales:** Dejar en blanco
- **Apellidos:** Apellidos del usuario
- **Nombre completo:** Este campo se llenará automáticamente con el contenido del campo **Nombre de pila** mas el contenido del campo **Apellidos**
- **Nombre de inicio de sesión de usuario:** este es el nombre que el usuario deberá utilizar para iniciar sesión en cualquier equipo que forme parte del dominio, escribir este campo siempre con letras minúsculas.
- **Nombre de inicio de sesión de usuario (anterior a Windows 2000):** Este campo se llenará automáticamente con el contenido del campo anterior.



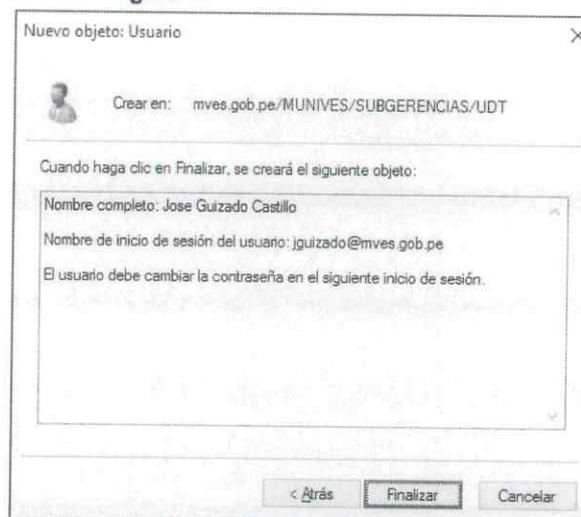

	MUNICIPALIDAD DE VILLA EL SALVADOR	Año: 2022
	POLITICAS DE SEGURIDAD DE LA INFORMACION	Versión: 1.0
		Página: 57 de 72

Luego de haber llenado los campos hacer clic en el botón “**Siguiente**”

- En la siguiente ventana se deberá escribir la **contraseña** del nuevo usuario, dicha contraseña deberá cumplir con los siguientes parámetros:
 - Debe tener al menos **7 caracteres (letras, números o símbolos)**
 - Debe tener al menos **una letra mayúscula**
 - Debe tener al menos **una letra minúscula**
 - Debe tener al menos **un número**.
 - No debe contener o ser igual al contenido de los campos **Nombre de pila o Apellidos**.
 - No debe contener o ser igual al contenido del campo **nombre de inicio de sesión de usuario**.



- Dejar habilitada la opción “**El usuario debe cambiar la contraseña en el siguiente inicio de sesión**”, esto con el fin de que el usuario tenga que cambiar obligatoriamente la contraseña inicial que le hemos asignado inicialmente en el momento en el que vaya a utilizar sus credenciales de dominio por primera vez en cualquier equipo del dominio.
- Luego hacer clic en el botón “**Siguiente**”.



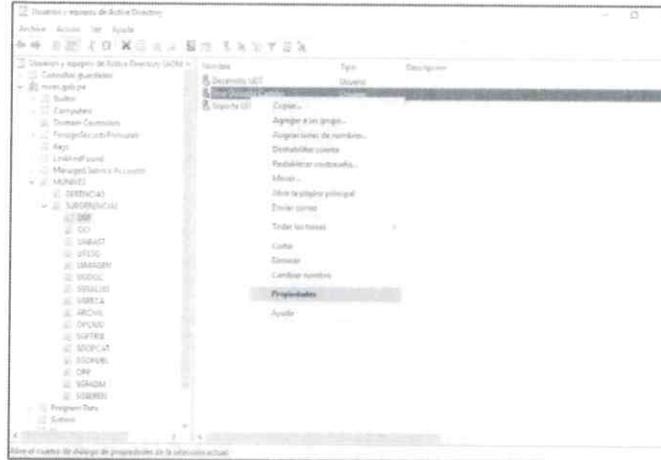

Finalmente se mostrará una ventana en cual confirmaremos la creación del usuario haciendo clic en el botón **Finalizar**.

De esta forma hemos creado una nueva cuenta de usuario de dominio en una unidad organizativa.

	MUNICIPALIDAD DE VILLA EL SALVADOR	Año: 2022
	POLITICAS DE SEGURIDAD DE LA INFORMACION	Versión: 1.0
		Página: 58 de 72

Para Agregar información adicional una cuenta de usuario:

1. Haga clic con el botón secundario del mouse en el objeto usuario y luego en el menú haga clic en la opción "Propiedades".



2. En la ventana "Propiedades: Nombre de Usuario", se podrán agregar o modificar datos de la cuenta del usuario, así como consultar información respectiva a una determinada cuenta de usuario dentro del dominio, se recuerda que siempre se debe tener bastante cuidado al intentar modificar cualquier dato en dichas opciones:



3. Luego de haber agregado los datos respectivos o haber realizado alguna modificación en la cuenta de usuario, hacer clic en el botón Aplicar y Luego hacer clic en el botón Aceptar.



6.1.7 Actividades Administrativas Básicas En Un Red Administrada Por Un Dominio Active Directory:

- Agregar Equipos al dominio
- Restablecer contraseñas de usuarios de dominio
- Deshabilitar usuarios del dominio

6.1.7.1 Agregar Equipos al dominio munives:

Para agregar un equipo al dominio “munives” se deberá proceder con los siguientes pasos:

Paso N°1: Configuración de DNS del dominio en el equipo:

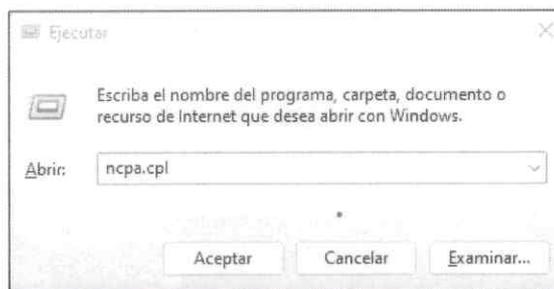
- Iniciar sesión en el computador con el usuario **Administrador local** del equipo:



- Una vez se muestre el escritorio de Windows, deberemos presionar al mismo tiempo en el teclado de la computadora las teclas:  +  (ambas teclas resaltadas en rojo en la siguiente imagen)



- Como resultado de esta acción se mostrará la ventana **Ejecutar**, aquí en el cuadro de texto “Abrir” deberemos escribir el comando “ncpa.cpl” sin las comillas como muestra la imagen que esta debajo y luego hacer clic en el botón **Aceptar**:



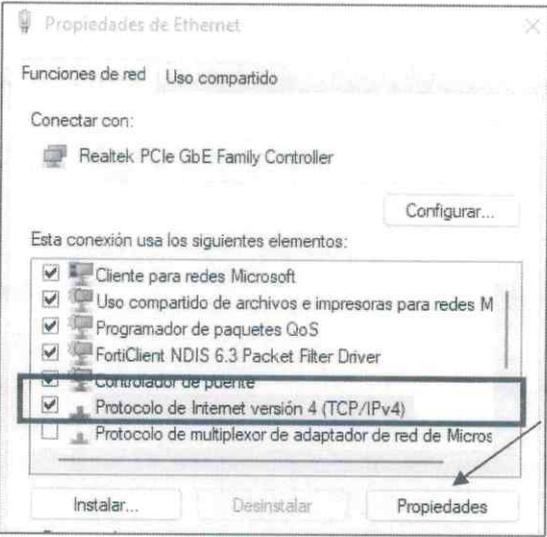
- Como resultado de esta acción se mostrará la ventana de **Conexiones de red**, aquí hacemos clic en la conexión de red principal del equipo, en este caso la conexión tiene el nombre **“Conexión de área local”** como muestra la siguiente imagen:



- Una vez seleccionada la conexión, hacemos clic sobre ella con el botón secundario del mouse y en las opciones que nos aparecen, hacemos clic en la que dice **“Propiedades”** como muestra la siguiente imagen:

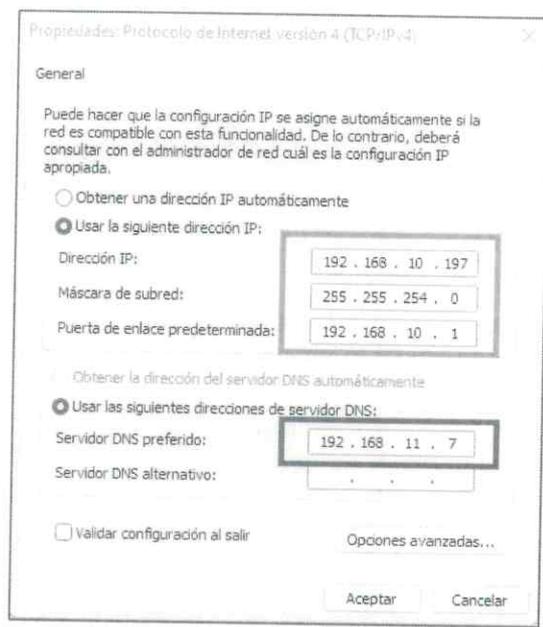


Como resultado de esta acción se mostrará la ventana **“Propiedades de Conexión de área Local”**, aquí debemos hacer doble clic sobre **“Protocolo de Internet versión 4 (TCP / IPv4)”** resaltada en rojo en la siguiente imagen:





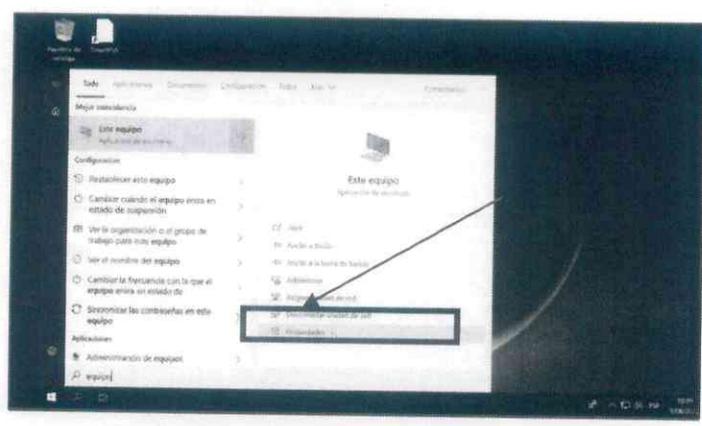
- Se mostrará la ventana para configurar el direccionamiento IP del equipo, aquí deberemos tener en cuenta que independientemente de la **Dirección IP / Mascara de subred / Puerta de enlace predeterminada** del equipo en la red del local municipal donde se encuentre funcionando (resaltado en azul), se deberá configurar como **Servidor DNS preferido** a la IP del controlador dominio principal a la IP: **192.168.11.7** (Resaltada en rojo en la imagen)



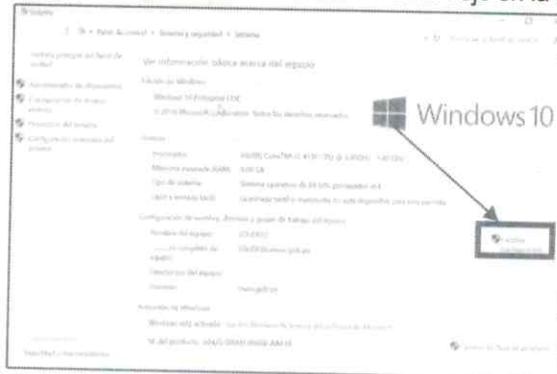
- Esta configuración permitirá que el equipo pueda encontrar el controlador de dominio al momento que procedamos a agregarlo al dominio "munives", del mismo modo habilitara la resolución de nombres dentro de la red a través del servicio DNS instalado en el controlador de dominio principal.
- Finalmente hacemos clic en el botón Aceptar para aplicar la nueva configuración.

Paso N° 2: Agregar el equipo al dominio

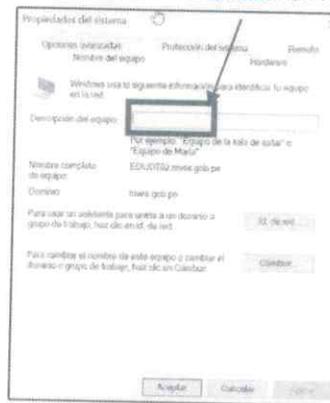
- Solo después de haber completado el paso N° 1, procederemos a agregar el equipo al dominio haciendo clic en el botón "Inicio", luego buscar la opción "Equipo" y hacer clic con el botón secundario del mouse sobre dicha opción, luego en el menú desplegable haremos clic en la opción "Propiedades" como muestra la siguiente imagen:



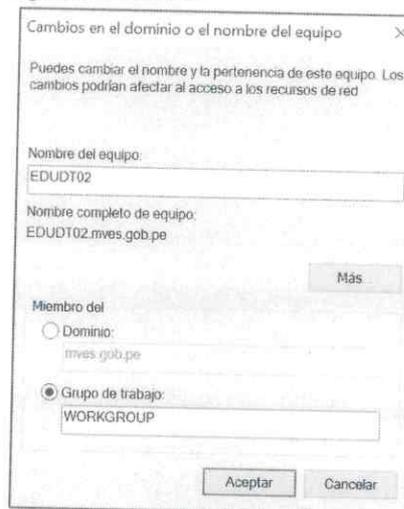
- Como resultado de esto se mostrará la ventana “Sistema”, en esta ventana debemos de hacer clic en la opción “**Cambiar configuración**” resaltada en color rojo en la siguiente imagen:



- A continuación, en la ventana “**Propiedades del sistema**”, dentro de la ficha “**Nombre de equipo**”, haremos clic en el botón “**Cambiar...**” resaltado en rojo en la siguiente imagen:

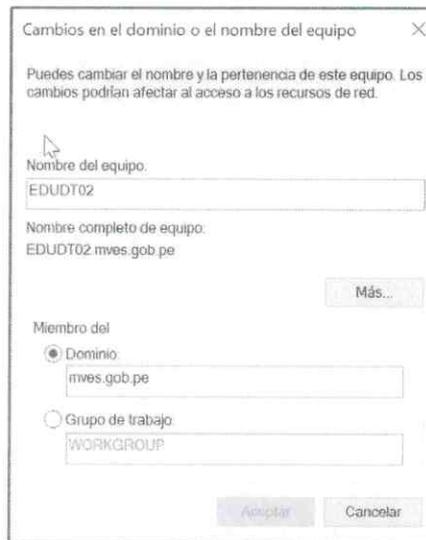


- Se mostrará en pantalla la siguiente ventana:

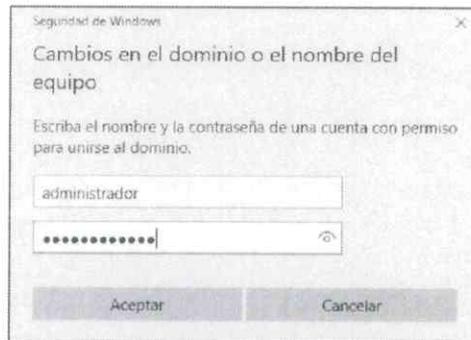


- Esta ventana nos va a permitir agregar el equipo del dominio “**mves**”, seleccionamos la opción (*) Dominio y en el cuadro de texto correspondiente escribimos “**mves**”, luego hacemos clic en el botón **Aceptar**.

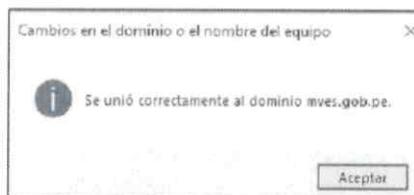
	MUNICIPALIDAD DE VILLA EL SALVADOR	Año: 2022
	POLITICAS DE SEGURIDAD DE LA INFORMACION	Versión: 1.0
		Página: 63 de 72



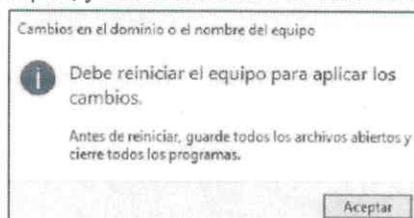
- Como resultado de esta acción nos aparece la ventana **"Seguridad de Windows"**, en el cuadro de texto "Nombre de usuario" debemos escribir el nombre de inicio de sesión de una cuenta de un usuario del dominio con permisos para agregar equipos al dominio, en este caso utilizaremos las credenciales del usuario **"soporte"**, y luego hacemos clic en el botón **Aceptar**.



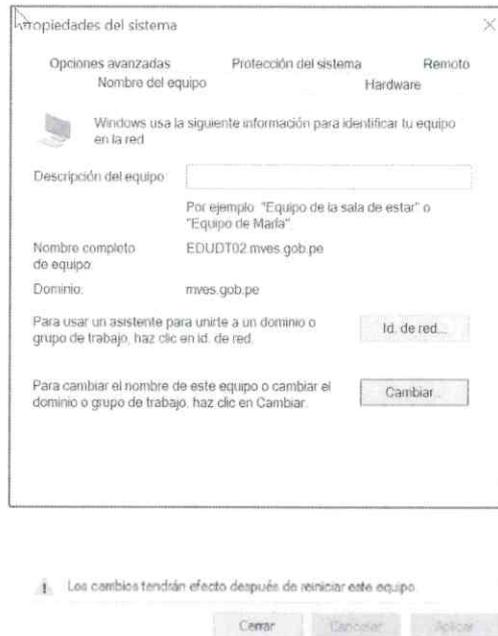
- Si todos los pasos anteriores fueron realizados de forma correcta, se deberá mostrar un mensaje de notificación similar a este indicando que el equipo se unió correctamente a nuestro dominio.



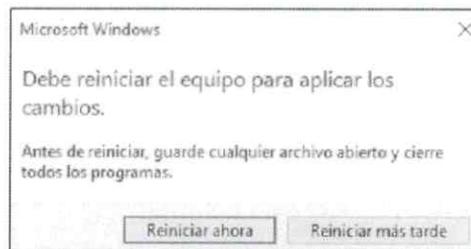
- Haremos clic en el botón **Aceptar**, y se mostrara una ventana similar a esta:



- Hacemos clic nuevamente en el botón **Aceptar**, luego en la ventana **“Propiedades del sistema”** hacemos clic en el botón **Cerrar**, como muestra la siguiente imagen:



- Como resultado de esta acción se mostrará una ventana de confirmación indicándonos que se debe reiniciar el equipo para completar los cambios en la configuración del equipo, hacemos clic en el botón **Reiniciar ahora**, para reiniciar el equipo.



- Después de que el equipo que se acaba de agregar al dominio haya reiniciado, se mostrara una ventana similar a esta, donde daremos clic en **“Otro usuario”**:

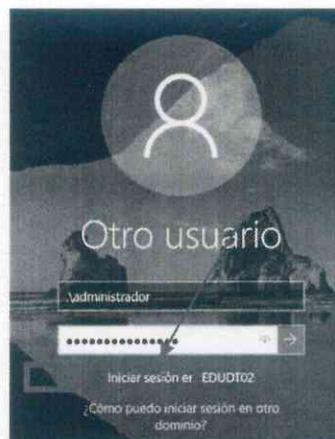


	MUNICIPALIDAD DE VILLA EL SALVADOR	Año: 2022
	POLITICAS DE SEGURIDAD DE LA INFORMACION	Versión: 1.0
		Página: 65 de 72

- Como resultado de esta acción se mostrará dos cuadros de texto, uno para ingresar el nombre de inicio de sesión de usuario del dominio **"munives"** con el que deseamos iniciar sesión en el equipo con su respectiva contraseña, y luego presionar la tecla **"Enter"** en el teclado del equipo o **hacer clic en la flecha resaltada en rojo en la imagen:**



- Como resultado de esta acción deberá completarse el inicio de sesión de nuestro usuario de dominio en el equipo mostrándonos el escritorio de Windows.
- Adicionalmente, se recuerda que una vez que un equipo ha sido agregado a un dominio de Active Directory, para poder iniciar una sesión **con cuentas de usuario locales del equipo**, será necesario anteponer los caracteres **“.”** **al nombre del usuario local** con el que se desea iniciar sesión en el equipo, por ejemplo como en el caso que sea necesario iniciar sesión con el usuario **Administrador Local del equipo**, con el fin de **identificar a los usuarios locales que pudiera tener el equipo o restablecer sus contraseñas**, como se muestra en la siguiente imagen:



- Como se resalta en rojo en la imagen se estaría iniciando sesión con un usuario local del equipo **"EDUDT02"** y no en el dominio **"MVES"**.

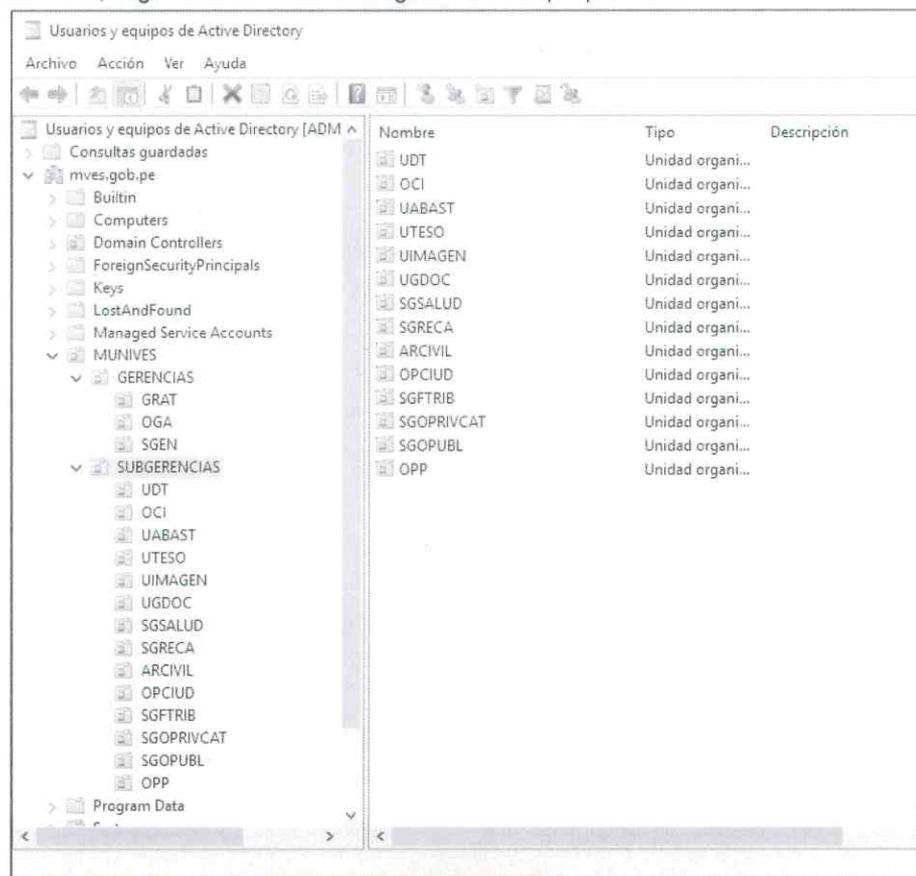
6.1.7.2 Restablecer contraseñas de usuarios de dominio

- Una de las tareas más básicas de la administración de los usuarios de un dominio Active Directory es el restablecimiento de contraseñas de los usuarios, para proceder con esta tarea será necesario ingresar por escritorio remoto nuevamente al controlador de dominio principal

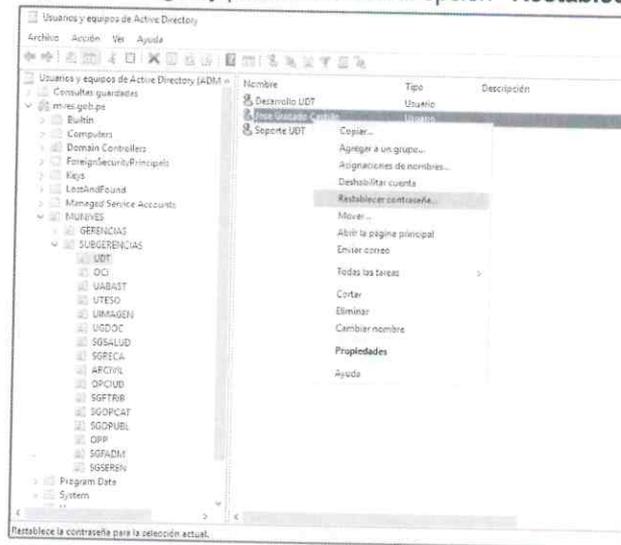
con las credenciales del usuario **Administrador del dominio**, y una vez allí ingresaremos a la consola de Administración **“Usuarios y equipos de Active Directory”**.



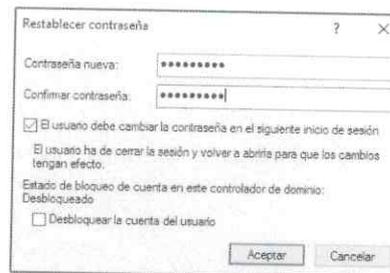
- Una vez dentro de la consola en el panel de objetos del lado izquierdo de la consola seleccionamos la **Unidad Organizativa** principal llama **“MUNIVES”**, y luego buscamos de acuerdo a la unidad orgánica a la que pertenece el usuario al que deseamos resetearle la contraseña, según a la Gerencia o Subgerencia a la que pertenezca:



- Una vez que hallemos al usuario al que queremos resetearle la contraseña hacemos clic con el botón secundario del mouse sobre el objeto usuario correspondiente del panel derecho como muestra la siguiente imagen y |seleccionamos la opción **“Restablecer contraseña...”**



- Nos aparecerá la siguiente ventana que nos permitirá restablecer la contraseña del usuario seleccionado:

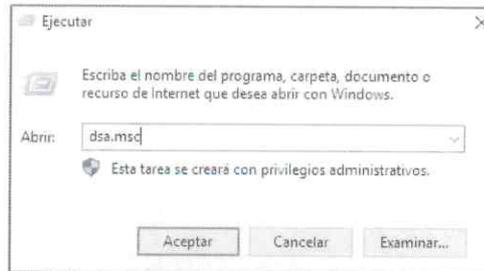


- En esta ventana deberemos ingresar la contraseña nueva para el usuario que hemos seleccionado en el cuadro de texto **“Contraseña nueva”**, y luego volver a escribir exactamente igual la misma nueva contraseña en el cuadro de texto **“Confirmar contraseña”**, de acuerdo a los siguientes parámetros establecidos:
 - ✓ La contraseña debe tener al menos 7 caracteres (letras, números o símbolos)
 - ✓ La contraseña debe tener al menos una letra mayúscula
 - ✓ La contraseña debe tener al menos una letra minúscula
 - ✓ La contraseña debe tener al menos un número.
 - ✓ La contraseña no debe contener o ser igual al contenido de los campos Nombre de pila o Apellidos del usuario
 - ✓ La contraseña no debe contener o ser igual al contenido del campo nombre de inicio de sesión del usuario.
- Tener en cuenta siempre que si se deja activada la opción **“El usuario debe cambiar la contraseña en el siguiente inicio de sesión”**, al momento que el usuario intente iniciar sesión en un equipo del dominio, se le solicitara automáticamente el cambio de contraseña antes de iniciar sesión en el equipo.



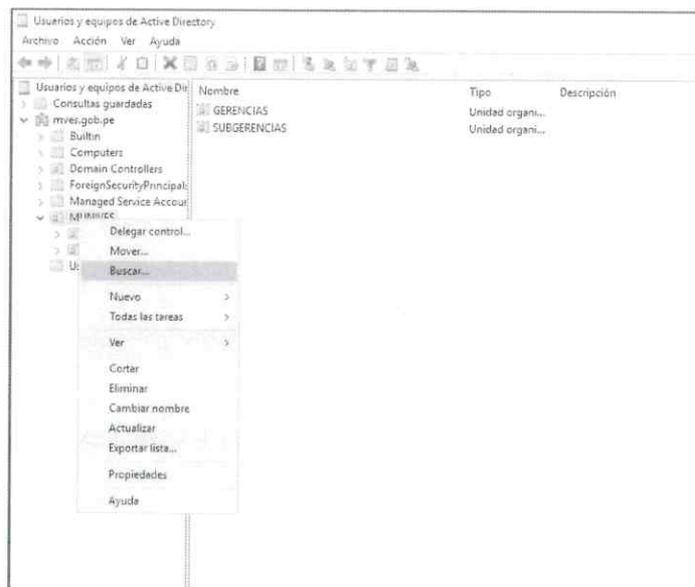
6.1.7.3 Deshabilitar usuarios del dominio

- Para deshabilitar uno o mas usuarios de dominio será necesario ingresar nuevamente de forma remota al servidor controlador de dominio principal (**192.168.11.7**) con las credenciales del usuario **Administrador del dominio** y una vez dentro del servidor, ejecutar la consola **“Usuarios y Equipos de Active Directory”**, escribiendo el comando **“dsa.msc”** sin las comillas en la ventana **“Ejecutar”** presionando las combinaciones de teclas: Windows + R como muestra la siguiente imagen:

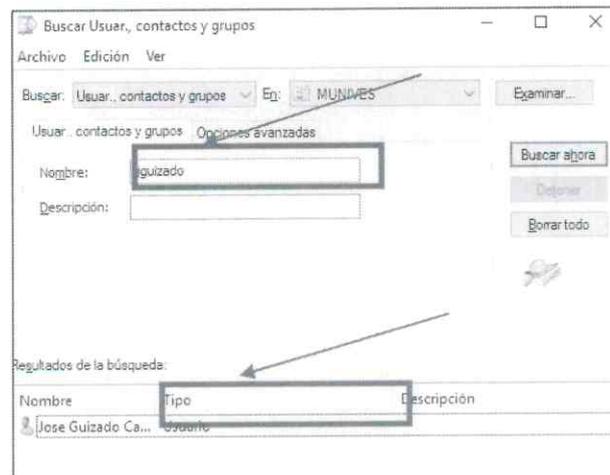


Y haciendo clic en el botón **Aceptar** o Presionamos la Tecla Enter en el teclado del equipo.

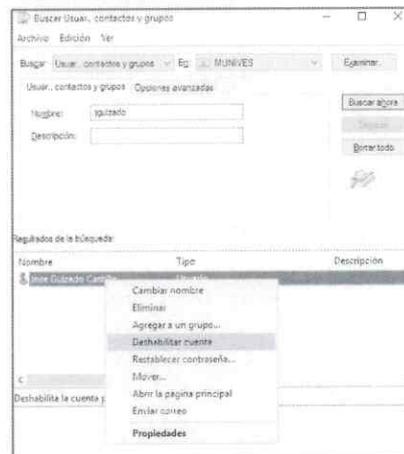
- Una vez dentro de la consola, procederemos a localizar al usuario a deshabilitar utilizando la opción buscar en todo el dominio **“mves.gob.pe”**, seleccionando dicho objeto que se encuentra en el panel izquierdo de la consola, y haciendo clic con el botón secundario del mouse sobre él, y seleccionamos la opción **Buscar** y hacemos clic en ella:



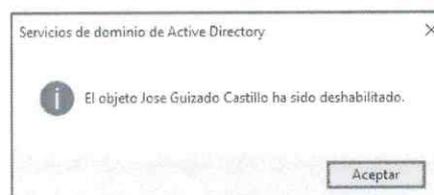
- Una vez dentro de la ventana **Buscar**, como muestra la imagen escribimos en el cuadro de texto **“Nombre”** el nombre o apellidos ó nombre de inicio de sesión del usuario que deseamos deshabilitar, luego hacemos clic en el botón **“Buscar ahora”** sombreado en azul en la imagen, esperamos un instante y si hemos escrito correctamente los datos del usuario nos mostrara el resultado de la búsqueda en la parte inferior donde dice **“Resultados de la búsqueda”**, en el ejemplo ha encontrado un usuario el cual se muestra resaltado en amarillo en la imagen:



- A continuación, seleccionamos la cuenta de usuario localizada como resultado de la búsqueda, y hacemos clic sobre ella con el botón secundario del mouse, luego seleccionamos la opción **“Deshabilitar cuenta”**

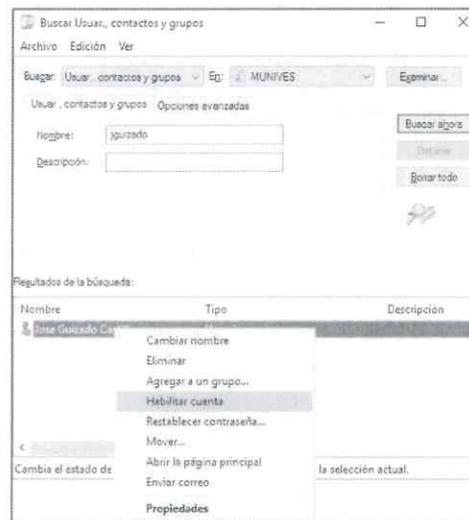


- Como resultado de esta acción se mostrará una ventana de notificaciones indicándonos que el usuario ha sido deshabilitado del dominio, esto tendrá como efecto que dicho usuario **no podrá iniciar sesión en ninguno de los equipos que forman parte del dominio “munives”**.



- En el caso contrario que deseemos **habilitar** algún usuario **deshabilitado**, simplemente seguimos los mismos pasos anteriores para encontrarlo y seleccionamos el usuario nuevamente haciendo clic secundario sobre el usuario que deseamos habilitar, y elegimos la opción **“Habilitar cuenta”**





- Como resultado de esta acción se mostrará la siguiente ventana de notificación:



7. Recomendaciones Finales:

- Se recomienda en primera instancia la implementación de un **servidor controlador de dominio secundario** en otro servidor físico diferente del equipo servidor donde se encuentra alojado el servidor controlador de dominio principal, esto con la finalidad de **garantizar la operatividad de la infraestructura del dominio Active Directory “ en caso de un fallo crítico en el servidor físico y/o virtualizado que aloja actualmente al controlador de dominio principal que pudiera interrumpir la continuidad del servicio.**
- Se recomienda la implementación del servicio **DHCP** (Protocolo de configuración dinámica de host) en la medida de lo posible en cada una de las redes LAN correspondientes a cada local municipal con el fin facilitar la autoconfiguración del direccionamiento IP en los equipos de computo que se conectan a la red municipal, esto con el fin de facilitar el acceso para los usuarios a la red y facilitar la configuración de los equipos al personal de soporte de la UDT.
- Se recomienda la implementación de una solución **SAN (Storage Area Network)** para la **centralización, seguridad y fiabilidad del almacenamiento de los archivos compartidos y almacenados por las diferentes unidades orgánicas de la municipalidad de Villa El Salvador** que se encuentran actualmente alojados en discos duros **NAS**, así como para el respaldo automatizado periódico y basado en políticas de backup establecidas previamente en coordinación con la subgerencia de la UDT.



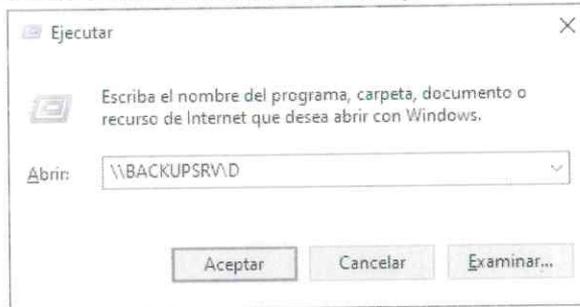


Anexo Nro.06 : “Manual Interno de Recuperación de Información del SIAF”

En un servidor con Windows Server de 64 Bits correctamente instalado se procede de la siguiente manera:

- 1. Se procede a buscar el último Backup del Sistema correspondiente del día anterior.

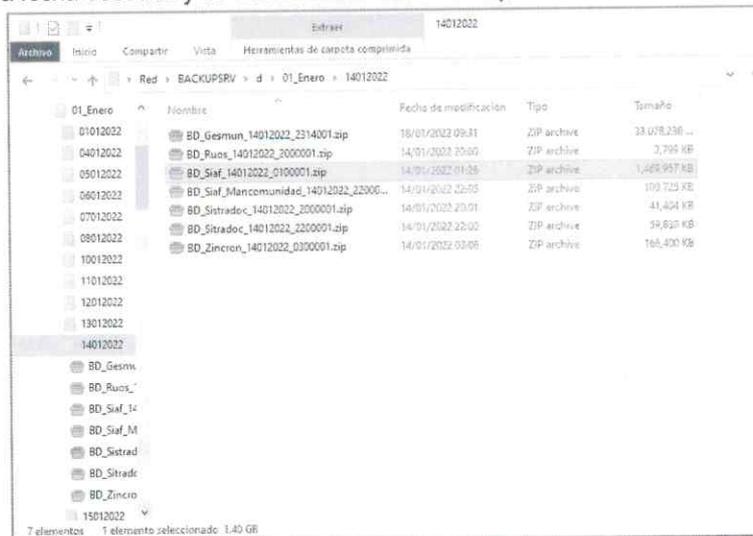
- o Ingresamos a la siguiente ruta donde se encuentra los Backup:



- o Se selecciona la carpeta deseada (los Backup están organizados por mes) y se ingresa.



- o Se selecciona la fecha deseada y se selecciona la data a recuperar.



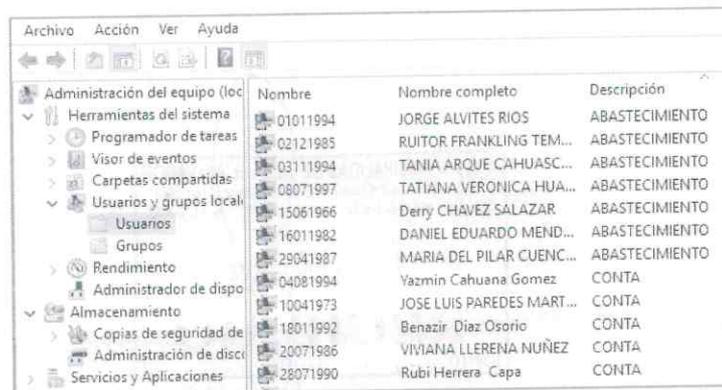
- o Se copia el Backup deseado, para restaurarlo.



- Se procede descomprimir y copiar el Backup a la carpeta:
D:\ Siaf_gl\$



- Se procede a crear los usuarios del Servidor que tendrán acceso a la carpeta D:\siaf_presupuesto



- Se configura como unidad de Red M a la carpeta D:\ Siaf_gl\$



- Se instala las librerías e instaladores del sistema

