

 Municipalidad de La Punta	DIRECTIVA DE ÓRGANO: “DIRECTIVA DE ÓRGANO DE SEGURIDAD DE LA INFORMACIÓN PARA LA MUNICIPALIDAD DISTRITAL DE LA PUNTA.”	RESOLUCIÓN DE ADMINISTRACIÓN	
		N° 110-2024-MDLP/OGA	20 de noviembre del 2024

MUNICIPALIDAD DISTRITAL DE LA PUNTA
Oficina General de Administración



DIRECTIVA DE ÓRGANO N° 006-2024-MDLP/OGA “DIRECTIVA DE ÓRGANO DE SEGURIDAD DE LA INFORMACIÓN PARA LA MUNICIPALIDAD DISTRITAL DE LA PUNTA.”
--



LA PUNTA, 2024

Municipalidad Distrital de La Punta	Página 1 de 11
Oficina General de Administración	

 Municipalidad de La Punta	DIRECTIVA DE ÓRGANO: "DIRECTIVA DE ÓRGANO DE SEGURIDAD DE LA INFORMACIÓN PARA LA MUNICIPALIDAD DISTRITAL DE LA PUNTA."	RESOLUCIÓN DE ADMINISTRACIÓN	
		Nº 110-2024-MDLP/OGA	20 de noviembre del 2024

CONTENIDO

1. FINALIDAD	3
2. OBJETIVO	3
3. BASE LEGAL	3
4. ALCANCE	4
5. RESPONSABILIDAD	4
6. DISPOSICIONES GENERALES	4
7. DISPOSICIONES ESPECÍFICAS.....	5
8. DISPOSICIONES COMPLEMENTARIAS.....	9
9. GLOSARIO DE TÉRMINOS.....	9
10. ANEXOS	11



 Municipalidad de La Punta	DIRECTIVA DE ÓRGANO: "DIRECTIVA DE ÓRGANO DE SEGURIDAD DE LA INFORMACIÓN PARA LA MUNICIPALIDAD DISTRITAL DE LA PUNTA."	RESOLUCIÓN DE ADMINISTRACIÓN	
		N° 110-2024-MDLP/OGA	20 de noviembre del 2024

DIRECTIVA DE ÓRGANO DE SEGURIDAD DE LA INFORMACIÓN PARA LA MUNICIPALIDAD DISTRITAL DE LA PUNTA

1. FINALIDAD

Contar con un documento de gestión aprobado que establezca lineamientos y controles de seguridad de la información institucional oficial de la Entidad, tanto en proceso como final, garantizando el cumplimiento normativo en el ámbito informático.

2. OBJETIVO

Mitigar los riesgos de pérdida de información, y proteger adecuadamente los recursos informáticos de la Municipalidad Distrital de La Punta, enfocado a asegurar la confidencialidad, integridad y disponibilidad de la información institucional.

3. BASE LEGAL

- 3.1. Decreto Supremo N°004-2019-JUS, Decreto Supremo que aprueba el Texto Único Ordenado de la Ley N°27444 – Ley de Procedimiento Administrativo General.
- 3.2. Decreto de Urgencia N°007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
- 3.3. Decreto Supremo N°029-2021-PCM, Decreto Supremo que aprueba el Reglamento del Decreto Legislativo N°1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.
- 3.4. 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.
- 3.5. Resolución de Secretaría de Gobierno y Transformación Digital N°002-2023-PCM/SGTD, aprueban la directiva N°001-2023-PCM/SGTD, Directiva que establece el perfil y responsabilidades del Oficial de Seguridad y Confianza Digital.
- 3.6. Ordenanza N°004-2023-MDLP/AL, ordenanza que aprueba el nuevo Reglamento de Organización y Funciones (ROF) y la Estructura Orgánica de la Municipalidad Distrital de La Punta, y sus modificaciones.
- 3.7. Resolución de Alcaldía N° 077-2023-MDLP/AL, que designa al Sr. Percy Condori Condori, como Oficial de Seguridad y Confianza Digital de la Municipalidad Distrital de La Punta.
- 3.8. Resolución de Alcaldía N° 093-2023-MDLP/AL, que conforma el Equipo de Respuestas ante Incidentes de Seguridad Digital de la Municipalidad Distrital de La Punta.
- 3.9. Resolución de Alcaldía N° 021-2024-MDLP/AL, que aprueba la actualización de la conformación del Comité de Gobierno y Transformación Digital de la Municipalidad Distrital de La Punta.



 Municipalidad de La Punta	DIRECTIVA DE ÓRGANO: "DIRECTIVA DE ÓRGANO DE SEGURIDAD DE LA INFORMACIÓN PARA LA MUNICIPALIDAD DISTRITAL DE LA PUNTA."	RESOLUCIÓN DE ADMINISTRACIÓN	
		N° 110-2024-MDLP/OGA	20 de noviembre del 2024

4. ALCANCE

Las disposiciones contenidas en la presente Directiva son de cumplimiento para todos los usuarios que hacen uso de los recursos informáticos de la Municipalidad Distrital de La Punta (MDLP).

5. RESPONSABILIDAD

- 5.1. La Oficina de Tecnologías de la Información (OTI) de la Oficina General de Administración (OGA) es el órgano responsable del cumplimiento de las disposiciones contenidas en la presente Directiva.
- 5.2. El Oficial de Seguridad y Confianza Digital de la OTI, es el responsable de informar a la Oficina General de Administración de las incidencias de seguridad informática, así como supervisar el cumplimiento de la siguiente directiva y mantener una documentación detallada sobre los controles de seguridad de la información.
- 5.3. El Comité de Gobierno y Transformación Digital de la entidad, es responsable de promover la gestión de seguridad de la información en los procesos y cultura organizacional de la entidad.
- 5.4. El Administrador de Red de la Oficina de Tecnologías de la Información es responsable de implementar las medidas de control para prevenir y detectar los accesos no autorizados a los recursos informáticos; asimismo, gestionar la atención de accesos a cuentas de red, aplicaciones, internet y servicios de la nube.
- 5.5. Los órganos y las unidades orgánicas de la MDLP deben velar por el uso autorizado de los recursos informáticos realizados por servidores públicos, locadores de servicios, proveedores y practicantes de sus respectivas unidades de organización.
- 5.6. Los servidores públicos de la MDLP, independientemente de la modalidad de contratación, son responsables de cumplir con el uso autorizado de los recursos informáticos.
- 5.7. Los jefes de los órganos y/o unidades orgánicas son los responsables de la presentación, así como de brindar su conformidad a los pedidos de accesos a recursos informáticos.
- 5.8. El Equipo de Respuestas ante Incidentes de Seguridad Digital de la OTI es responsable de efectuar la respuesta o recuperación ante los incidentes de seguridad digital que afectan los activos de la MDLP.

6. DISPOSICIONES GENERALES

- 6.1. La Oficina General de Administración a través de la Oficina de Tecnologías de la Información es la encargada de garantizar la confidencialidad, integridad y disponibilidad de la información institucional administrada por los sistemas de información.
- 6.2. El Oficial de Seguridad y Confianza Digital es el encargado de coordinar con los jefes de los órganos o unidades orgánicas la gestión de riesgos e implementación de los controles de seguridad de la información identificados en sus ámbitos de competencia, así como brindar apoyo en la gestión de incidentes de seguridad de la información al Equipo de Respuesta a Incidentes de Seguridad de la información.



 Municipalidad de La Punta	DIRECTIVA DE ÓRGANO: "DIRECTIVA DE ÓRGANO DE SEGURIDAD DE LA INFORMACIÓN PARA LA MUNICIPALIDAD DISTRITAL DE LA PUNTA."	RESOLUCIÓN DE ADMINISTRACIÓN	
		N° 110-2024-MDLP/OGA	20 de noviembre del 2024

- 6.3. Todos los órganos y unidades orgánicas de la MDLP deben de cumplir y/o implementar, en el ámbito de su competencia; los lineamientos de seguridad de la información establecidos en la presente directiva.
- 6.4. Todos los servidores civiles deben cumplir con los lineamientos de seguridad de la información establecidos en esta Directiva y de manera excepcional, los locadores de servicio cuando sean requeridos por el área usuaria, para el cumplimiento de sus funciones también deberán adherirse a estos lineamientos al tratar la información de la entidad.

7. DISPOSICIONES ESPECÍFICAS

A. MEDIDAS DE CONTROL PARA LA SEGURIDAD INFORMÁTICA

7.1. Seguridad Física al Centro de Datos y Recursos Informáticos.

- 7.1.1. Acceso al Centro de Datos: Con la finalidad de controlar y restringir el acceso al Centro de Datos por la Oficina de Tecnologías de la Información, se establece lo siguiente:
- a. El Administrador de Red de la OTI otorga los pases de accesos para los siguientes casos:
- i. Pase permanente: Se otorga el acceso permanente al personal, que por la naturaleza de sus funciones ingresa a los ambientes del Centro de Datos.
- ii. Pase temporal: Se otorga de manera excepcional al usuario, a solicitud del jefe del órgano o unidad orgánica, mediante documento formal dirigido a la Oficina de Tecnologías de la Información (OTI), justificando los motivos, para su evaluación y otorgamiento de la autorización. Asimismo, el usuario es responsable por el uso correcto del pase temporal sin alterar la integridad de los equipos y/o la información contenida.

- 7.1.2. Acceso a los recursos informáticos del Centro de Datos: El Administrador de Red de la OTI, autoriza el acceso a los recursos informáticos y de comunicaciones que se encuentran en el Centro de Datos, a solicitud del jefe del órgano o unidad orgánica, mediante documento formal dirigido a la OTI, justificando los motivos para acceder a estos recursos, además, debe precisar el nombre de los usuarios y el tiempo de vigencia para dichos accesos. Asimismo, el usuario debe hacer el uso correcto de los accesos sin alterar la integridad de los recursos informáticos y/o de su información contenida.

7.2. Seguridad Perimetral de la Plataforma Tecnológica de la MDLP.

- 7.2.1. Protección de la puerta de enlace: El Administrador de Red de la OTI, de acuerdo con la disponibilidad de recursos y la capacidad tecnológica instalada, implementa las medidas de control para prevenir el acceso de atacantes digitales a la red de datos de la MDLP. Estas medidas preferentemente son: Firewall, programas antimalware u otras que se defina.
- 7.2.2. Protección en los Endpoint: El Administrador de Red de la OTI de acuerdo con la disponibilidad de recursos y la capacidad tecnológica instalada, implementa

 Municipalidad de La Punta	DIRECTIVA DE ÓRGANO: "DIRECTIVA DE ÓRGANO DE SEGURIDAD DE LA INFORMACIÓN PARA LA MUNICIPALIDAD DISTRITAL DE LA PUNTA."	RESOLUCIÓN DE ADMINISTRACIÓN	
		N° 110-2024-MDLP/OGA	20 de noviembre del 2024

las medidas de detección y eliminación de malware o código malicioso. Estas medidas preferentemente son: Firewall, software antimalware y/u otras que se defina.

7.3. Seguridad en las Comunicaciones.

- 7.3.1. **Controles Criptográficos:** El Administrador de Red de la OTI, implementa mecanismos de encriptación para salvaguardar la transmisión de la información, considerando lo siguiente:
- a. En todas las comunicaciones hacia internet, implementa protocolos seguros de transferencia de hipertexto (HTTPS), a fin de mantener seguras dichas conexiones.
 - b. Mantiene actualizado los certificados de seguridad (SSL) mediante los cuales se protege la transmisión de información confidencial entre dos aplicaciones, los mismos que utilizan protocolos de seguridad (TLS).

7.4. Control de Cuentas de Usuario.

- 7.4.1. **Control de Cuentas:** Los usuarios que tienen una cuenta de acceso, deben cumplir con lo siguiente:
- a. Cuenta de usuario.
 - i. La cuenta de usuario y contraseña es de uso personal e intransferible, de manera única y exclusiva mientras dure el vínculo laboral o contractual con la MDLP.
 - ii. El usuario es responsable por el uso que se realicen con su cuenta de usuario.
 - iii. Cuando el usuario sospeche o compruebe que la seguridad de su contraseña pueda estar comprometida o haya sido vulnerada, debe reportar las incidencias de seguridad informática de inmediato mediante el correo electrónico seguridadoti@munilapunta.gob.pe para la evaluación correspondiente.
 - iv. Ante situaciones de sustracción o pérdida de información causados por la vulneración de la cuenta de usuario, el titular de la cuenta es responsable por los daños que se puedan causar a los recursos informáticos de la MDLP.
 - b. Cuenta de administrador.
 - i. El Administrador de Red, autoriza al personal los accesos a dichas cuentas, las mismas que deben contar con el visto bueno del jefe de la OTI.
 - ii. Mecanismos de control de contraseñas: El Administrador de Red de la OTI es el responsable de definir reglas para una adecuada generación de contraseñas para las cuentas de usuario.

 Municipalidad de La Punta	DIRECTIVA DE ÓRGANO: "DIRECTIVA DE ÓRGANO DE SEGURIDAD DE LA INFORMACIÓN PARA LA MUNICIPALIDAD DISTRITAL DE LA PUNTA."	RESOLUCIÓN DE ADMINISTRACIÓN	
		N° 110-2024-MDLP/OGA	20 de noviembre del 2024

7.5. Control de Servicios de Red y Aplicaciones.

7.5.1. **Acceso a los servicios de red:** Permite proteger la conexión de los usuarios a los servicios de red a través de los Endpoint, considerando lo siguiente:

- El jefe del órgano o unidad orgánica debe solicitar accesos a servicios de red para los usuarios de su unidad de organización.
- El Administrador de Red de la OTI, brinda los accesos a servicios de red otorgándoles una cuenta de usuario y contraseña para dicho fin.
- Los usuarios acceden a los servicios de red de datos a través de una cuenta de usuario y contraseña asignada.

7.5.2. **Accesos de la red externa a la red interna:** El control de acceso desde la red externa de la MDLP, permite asegurar la protección de accesos no deseados; considerando lo siguiente:

- Los usuarios solo pueden acceder a la red de datos interna de la MDLP, desde un enlace exterior, utilizando una conexión VPN (Red Privada Virtual) u otro mecanismo que defina el Administrador de Red de la Oficina de Tecnologías de la Información.
- El usuario que hace uso de la conexión VPN es responsable de las acciones que realice a través de este acceso remoto.

7.5.3. **Acceso a Internet:** Para el control de acceso a los servicios de internet se considera lo siguiente:

- El Administrador de Red de la OTI, establece los niveles de acceso a internet para acceder a través de la red de datos de la MDLP.
- Los accesos a internet son solicitados por el jefe del órgano o unidad orgánica y son otorgados de acuerdo con las disposiciones normativas de la OTI sobre atención de accesos a recursos de tecnologías de información.
- El usuario solo debe hacer uso de internet de manera única y exclusiva para el desarrollo de sus funciones y es responsable de las acciones que realice a través de los accesos otorgados.

7.5.4. **Acceso a los servicios de la nube:** Para el control de acceso a infraestructuras, plataformas o sistemas de software alojados por proveedores externos, que se ponen a disposición de los usuarios a través de Internet, se considera lo siguiente:

- Los accesos a los servicios de la nube son solicitados por el jefe del órgano o unidad orgánica, y son otorgados a los usuarios de su unidad de organización de acuerdo a la disponibilidad de los servicios en la nube establecida por la OTI.
- El usuario hace uso de los servicios de la nube de manera exclusiva para el desarrollo de sus funciones. Asimismo, tiene la obligación de responder por las acciones que se realicen con la cuenta asignada.

Municipalidad Distrital de La Punta

Oficina General de Administración

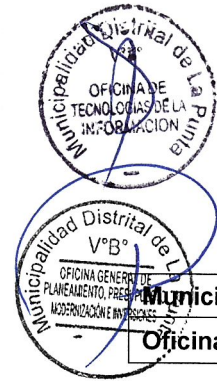
Página 7 de 11

 Municipalidad de La Punta	DIRECTIVA DE ÓRGANO: "DIRECTIVA DE ÓRGANO DE SEGURIDAD DE LA INFORMACIÓN PARA LA MUNICIPALIDAD DISTRITAL DE LA PUNTA."	RESOLUCIÓN DE ADMINISTRACIÓN	
		N° 110-2024-MDLP/OGA	20 de noviembre del 2024

- 7.5.5. **Acceso a las aplicaciones de la MDLP:** Para el control de acceso a las aplicaciones mediante el uso de las funcionalidades y acceso a la información contenida en las aplicaciones, se considera lo siguiente:
- a. Los accesos a las aplicaciones de la MDLP son solicitados por el jefe del órgano o unidad orgánica, y son otorgados a los usuarios de su unidad de organización de acuerdo con las disposiciones normativas de la OTI sobre atención de accesos a las aplicaciones.
 - b. El Administrador de Red de la OTI, brinda los accesos a las aplicaciones otorgándoles una cuenta de usuario y contraseña para dicho fin.
 - c. Los usuarios acceden a las aplicaciones de la MDLP a través de cuentas de usuario y contraseñas configuradas en el directorio activo del dominio de red o por mecanismos de seguridad de acceso propios de cada aplicación brindados por la OTI.
- 7.5.6. **Revisión de accesos a servicios de aplicaciones:** El jefe del órgano o unidad orgánica debe validar los accesos otorgados a los usuarios de su unidad de organización en coordinación con el Administrador de Red de la OTI.

B. GESTIÓN DE SEGURIDAD INFORMÁTICA

- 7.6. **Gestión de Vulnerabilidad de Seguridad Informática:** El Administrador de Red de la OTI realiza las pruebas de vulnerabilidad, emulando el comportamiento de un atacante digital de manera controlada a fin de verificar y evaluar la seguridad lógica de la plataforma tecnológica. De acuerdo con la disponibilidad de los recursos y a la capacidad tecnológica instalada en la OTI, podrá considerar las siguientes etapas para la gestión:
- 7.6.1. **Planificación y preparación:** Se establece un plan de ejecución definiendo el alcance y un cronograma de actividades.
 - 7.6.2. **Ejecución:** Se realizan rutinas de ataque ético utilizando las mismas técnicas y herramientas de un atacante digital real, con el fin de detectar debilidades de hardware y de software. Asimismo, se incluye el análisis de vulnerabilidad para las aplicaciones o sistemas de información que pueden efectuarse de manera independiente al plan de Ethical Hacking.
 - 7.6.3. **Comunicación:** Se elabora el informe de resultados para comunicar a los interesados y de ser necesario se implementa un plan de remediación.
 - 7.6.4. **Monitoreo:** Se realiza el seguimiento y actualización de los resultados de la ejecución del plan de remediación.
- 7.7. **Incidentes de Seguridad Informática:** La OTI gestiona las incidencias de seguridad informática a fin de controlar otros potenciales incidentes, y de ser necesario elabora un plan de acción para minimizar las ocurrencias y/o impacto en los recursos informáticos considerando lo siguiente:



 Municipalidad de La Punta	DIRECTIVA DE ÓRGANO: “DIRECTIVA DE ÓRGANO DE SEGURIDAD DE LA INFORMACIÓN PARA LA MUNICIPALIDAD DISTRITAL DE LA PUNTA.”	RESOLUCIÓN DE ADMINISTRACIÓN	
		N° 110-2024-MDLP/OGA	20 de noviembre del 2024

- 7.7.1. El usuario tiene la obligación de comunicar cualquier evento que incumpla las disposiciones normativas de la presente Directiva, mediante un mensaje de correo electrónico a la dirección seguridadoti@munilapunta.gob.pe.
- 7.7.2. El Oficial de Seguridad y Confianza Digital, identifica el problema y las deriva en caso corresponda a una incidencia de seguridad de la información al Administrador de Red, a fin de evaluarlas y de ser necesario elabora y ejecuta un plan de acción con el apoyo del Equipo de Respuestas ante incidentes de Seguridad Digital, para mitigar su ocurrencia y/o evitar su propagación y/o disminuir los daños a los recursos informáticos (contención, erradicación y recuperación).
- 7.7.3. El Oficial de Seguridad y Confianza Digital de la OTI notifica al órgano o unidad orgánica donde se presentó el evento, mediante documento formal, señalando los detalles del incumplimiento de las disposiciones de la presente Directiva, por parte de sus usuarios. Asimismo, realiza un informe a OGA detallando las recomendaciones y lecciones aprendidas.

El flujograma para el Procedimiento de Atención de Incidentes de Seguridad Informática, se encuentra en el Anexo 01.

8. DISPOSICIONES COMPLEMENTARIAS

- 8.1. El Oficial de Seguridad y Confianza Digital de la Oficina de Tecnologías de Información debe asegurar una comunicación efectiva de disposiciones de seguridad de la información a todos los servidores públicos.
- 8.2. El Oficial de Seguridad y Confianza Digital de la Oficina de Tecnologías de la Información debe realizar revisiones periódicas de esta directiva para adaptarlas a nuevos riesgos y cambios tecnológicos.

9. GLOSARIO DE TÉRMINOS

- 9.1. Aplicación: Un programa de software diseñado para ejecutar tareas específicas. Las aplicaciones pueden ser de propósito general o especializadas, y están diseñadas para interactuar con el usuario para cumplir una función concreta.
- 9.2. Atacante Digital: Individuo u organización que intenta obtener el acceso no autorizado a los recursos informáticos para utilizarlos con fines maliciosos como el robo, modificación y/o destrucción de la información.
- 9.3. Centro de Datos: Es un ambiente donde se concentran los servidores y recursos necesarios para el procesamiento y almacenamiento de la información con acceso restringido.
- 9.4. Cifrado: Es el proceso de conversión de datos mediante el uso de algoritmos y claves, de un formato legible a un formato codificado, con el fin de evitar accesos no autorizados.
- 9.5. Código Malicioso: Script informático dañino diseñado para crear vulnerabilidad en el sistema, que permita la generación de puertas traseras, brechas de seguridad, robo de información y datos; así como otros perjuicios potenciales en archivos y sistemas

 Municipalidad de La Punta	DIRECTIVA DE ÓRGANO: "DIRECTIVA DE ÓRGANO DE SEGURIDAD DE LA INFORMACIÓN PARA LA MUNICIPALIDAD DISTRITAL DE LA PUNTA."	RESOLUCIÓN DE ADMINISTRACIÓN	
		N° 110-2024-MDLP/OGA	20 de noviembre del 2024

informáticos.

- 9.6. Control de Acceso: Corresponde a los mecanismos para la identificación y autenticación, a fin de obtener autorización para acceder a los recursos informáticos a través de una cuenta de usuario. Asimismo, el acceso a los recursos informáticos es solicitado por el responsable de las unidades de organización y atendida de acuerdo con las disposiciones normativas internas de la Oficina de Tecnologías de la Información.
- 9.7. Criptográfico: Relativo a la criptografía, que corresponde a una técnica que protege la información de accesos no autorizados mediante la utilización del método de cifrado.
- 9.8. Cuenta de Usuario: Conjunto de datos, generalmente compuesto por un nombre de usuario y contraseña, que posibilitan el acceso a los recursos informáticos. Permiten la identificación del individuo como usuario del sistema y la autenticación o verificación de la identidad del individuo. Las cuentas de usuario son creadas para acceder a las computadoras de la red de la MDLP, a los servicios de impresoras, internet y al correo electrónico y aplicaciones.
- 9.9. Cuenta de Administrador: Es una cuenta de usuario que permite realizar cambios que afectan a otros usuarios. Los administradores pueden cambiar la configuración de seguridad del sistema, instalar software y hardware nuevos y acceder a todos los archivos del sistema.
- 9.10. Documento Formal: Escrito elaborado por el servidor público, persona autorizada de un proveedor de servicios o un locador de servicios, con valor oficial, legal y laboral para gestionar un trámite dentro de la entidad. Puede tratarse de memorando, informe, carta u oficio.
- 9.11. Endpoint: Dispositivos electrónicos en los que se almacena o procesa información de la Municipalidad Distrital de La Punta. Puede tratarse de servidores, estaciones de trabajo, celulares u otros.
- 9.12. Ethical Hacking: Corresponde a las pruebas de seguridad informática que ejecutan ataques digitales controlados a los recursos informáticos, con el fin de descubrir las vulnerabilidades de los servicios informáticos de la Oficina de Tecnologías de la Información (OTI).
- 9.13. Incidencias de Seguridad Informática: Impedimentos en la operación normal de los recursos informáticos, por el acceso, intento de acceso, uso, modificación o destrucción no autorizada de los recursos informáticos de la MDLP.
- 9.14. Malware: Software malicioso que cubre un amplio rango de software hostil, capaz de causar daños o alteraciones del sistema operativo, archivos, u otros componentes de computadoras y redes informáticas.
- 9.15. Propietario Funcional: Rol desempeñado por los servidores públicos de la MDLP, cuyas funciones son de solicitar y definir los requerimientos de servicios de TI de su unidad de organización, también de validar y aprobar las atenciones de sus requerimientos. Asimismo, es designado por el responsable de la unidad de organización mediante documento formal dirigido a la OTI.
- 9.16. Puerta de Enlace: Dispositivo dentro de una red informática, mediante el cual se permite el acceso a otra red. Es decir, sirve de enlace entre dos redes con protocolos y

 Municipalidad de La Punta	DIRECTIVA DE ÓRGANO: "DIRECTIVA DE ÓRGANO DE SEGURIDAD DE LA INFORMACIÓN PARA LA MUNICIPALIDAD DISTRITAL DE LA PUNTA."	RESOLUCIÓN DE ADMINISTRACIÓN	
		N° 110-2024-MDLP/OGA	20 de noviembre del 2024

arquitecturas diferentes. Su propósito fundamental es traducir la información del protocolo utilizado en una red, al protocolo en la red destino; también se le denomina Gateway.

- 9.17. Recursos Informáticos: Es el equipamiento de hardware y software interconectado para brindar los servicios informáticos, estos incluyen los medios para la entrada de datos, procesamiento, comunicación y almacenamiento de la información; asimismo, estos recursos están en custodia por la OTI.
- 9.18. Protocolo de Transparencia de Hipertexto Seguro (HTTPS): Protocolo de transparencia de hipertexto seguro que se utiliza para la comunicación en internet, cifra la información intercambiada entre el navegador web del usuario y el servidor, garantizando la confidencialidad y la integridad de los datos.
- 9.19. Red Privada Virtual (VPN): Tecnología de red que se utiliza para conectar de manera segura una o más computadoras a una red privada utilizando una red pública.
- 9.20. Seguridad informática: Conjunto de medidas técnicas destinadas a preservar la confidencialidad, integridad y disponibilidad de la información; pudiendo además abarcar otras propiedades como la autenticidad, la fiabilidad y el no repudio.
- 9.21. Seguridad perimetral: Conjunto de medidas utilizadas para proteger el acceso a los recursos tecnológicos a través de la puerta de enlace, mediante el uso firewalls, sistema de antivirus u otros existentes.
- 9.22. Secure Sockets Layer (SSL) (capa de conexión segura): Tecnología que utiliza un protocolo estándar de cifrado, a fin de mantener segura una conexión a Internet, protegiendo la información confidencial que se envía entre dos sistemas e impedir que el atacante digital acceda y modifique el dato que se transfiera.
- 9.23. Transport Layer Security (TLS) (seguridad de la capa de transporte): Protocolo estándar de cifrado que se utiliza para la transmisión de datos en internet. Es una versión actualizada y más segura de SSL.
- 9.24. Usuario: Servidor público, locador de servicio, proveedor y practicante, que hacen uso de los recursos informáticos de la Municipalidad Distrital de La Punta, debidamente autorizado/a según disposiciones emitidas por la Oficina de Tecnologías de la Información.
- 9.25. Vulnerabilidad: Corresponde a la debilidad encontrada en los recursos informáticos, que permite a un atacante digital comprometer la integridad, disponibilidad y/o confidencialidad de la información.

10. ANEXOS

- 10.1. Anexo 01: Flujograma del procedimiento para reportar Incidencias de Seguridad Informática en la MDLP.

ANEXO 01: FLUJOGRAMA DEL PROCEDIMIENTO PARA REPORTAR INCIDENCIAS DE SEGURIDAD INFORMÁTICA EN LA MDLP.

