Municipalidad de
La Punta

PLAN PREVENTIVO, DETECTIVO Y CORRECTIVO DE SEGURIDAD PARA CONTROLAR RIESGOS EN EL MANTENIMIENTO DE LOS SISTEMAS INFORMÁTICOS

Municipalidad Distrital de La Punta
OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

Municipalidad Distrital de La Punta
OFICINA GENERAL DE ADMINISTRACIÓN
OGA

Oficina de Tecnologías de la Información

2025 - 2027

	PLAN PREVENTIVO, DETECTIVO Y CORRECTIVO DE SEGURIDAD PARA CONTROLAR RIESGOS EN EL MANTENIMIENTO DE SISTEMAS INFORMÁTICOS

ROL	NOMBRE	UNIDAD / CARGO	FECHA	FIRMA
Elaborado por:	Percy German Condori Condori	OTI / JEFE DE OTI	01/06/2024	MUNICIPALIDAD DISTRITAL DE LA PUNTA PERCY GERMAN CONDORI CONDORI Jefe de la Oficina de Tecnologías de la Información

Municipalidad Distrital de La Punta
OFICINA DE TECNOLOGIAS DE LA INFORMACION

Municipalidad Distrital de La Punta
OFICINA GENERAL DE ADMINISTRACIÓN

CONTROL DE CAMBIOS

FECHA	VERSION	DESCRIPCIÓN	ELABORACIÓN	APROBACIÓN
01/06/2024	1.0.0	Creación del Documento	Percy German Condori Condori	MUNICIPALIDAD DISTRITAL DE LA PUNTA PERCY GERMAN CONDORI CONDORI Jefe de la Oficina de Tecnologías de la Información

INDICE

1. Introducción

La Municipalidad Distrital de La Punta, ha elaborado el Plan preventivo, detectivo y correctivo donde establece un conjunto los procedimientos esenciales para gestionar y mitigar los riesgos en el mantenimiento de sistemas informáticos. La elaboración del presente plan tiene como objetivo establecer las acciones orientadas a garantizar la seguridad y el funcionamiento óptimo de los sistemas informáticos de la entidad. La correcta implementación de este plan permitirá mitigar riesgos y asegurar la continuidad operativa.

2. Finalidad

Contar con un documento de gestión integral que defina planes de acción concretos orientados a prevenir incidentes de seguridad que puedan comprometer los sistemas informáticos de la Municipalidad Distrital de La Punta. Este plan busca establecer medidas para la detección temprana de vulnerabilidades y situaciones de riesgo, así como la corrección efectiva de fallos de seguridad que puedan afectar la disponibilidad, integridad y confidencialidad de la información crítica procesada y almacenada en los sistemas tecnológicos de la entidad asegurando así la continuidad operativa y el cumplimiento de normativas.

3. Objetivo

Garantizar la disponibilidad, integridad y confidencialidad de la información procesada y almacenada en los sistemas informáticos de la Municipalidad Distrital de La Punta, asegurando que esté protegida contra accesos no autorizados, modificaciones malintencionadas o pérdidas accidentales. Para lograr esto, se implementarán controles, políticas, procedimientos y tecnologías que permitan prevenir, detectar y responder de manera eficiente a amenazas y vulnerabilidades, garantizando la continuidad operativa y el cumplimiento de los estándares de seguridad establecidos.

4. Alcance

El presente Plan tiene como alcance tanto al personal de la Oficina de Tecnología de la Información (OTI), como a todos los funcionarios, directivos, servidores y locadores de servicios de la Municipalidad Distrital de La Punta que utilicen sistemas de información. Además, incluye los sistemas informáticos y componentes tecnológicos de la entidad, que deben ser objeto de las medidas preventivas, detectivas y correctivas para asegurar su correcta operación y protección ante riesgos de seguridad.

5. Marco Legal

El plan de seguridad se enmarca dentro de la legislación peruana aplicable a la gestión de sistemas informáticos y la protección de la información. Las normativas relevantes incluyen:

- Decreto Legislativo Nº1412, que aprueba la Ley de Gobierno Digital.
- Resolución Ministerial Nº004-2016-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.
- 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.
- Resolución de Gerencia Municipal Nº196-2018-MDLP/GM, que aprueba el Manual de Procedimiento (MAPRO) de la Oficina General de Administración.
- Resolución de la Oficina General de Administración Nº042-2017-MDLP/OGA, que aprueba la Directiva Nº10-2017-MDLP/OGA "Directiva Administrativa para el correcto uso de los equipos y sistemas informáticos de la Municipalidad Distrital de La Punta".

6. Duración del Plan

El presente Plan tendrá una vigencia de tres años del 2025 hasta el 2027. La duración del plan se ajustará según las evaluaciones periódicas y los resultados obtenidos durante su implementación, pudiendo ser revisado y actualizado según las necesidades cambiantes de la organización y la evolución de los sistemas informáticos

7. Infraestructura Tecnológica

7.1. Sistemas de Información

La Municipalidad Distrital de La Punta, cuenta con los siguientes sistemas de información clave que permiten la gestión y operación de los procesos administrativos, financieros, operativos y de control dentro de la organización.

SISTEMAS DE INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE LA PUNTA		
NOMBRE	**DESCRIPCIÓN**	**AREA USUARIA**
SISTEMA DE INFORMACIÓN DE GESTIÓN ADMINISTRATIVA - INTRASIG	Gestiona el personal y los trámites documentarios.	Todas las unidades orgánicas

SISTEMA DE RENTAS - GESMUN	Gestiona de manera eficiente y transparente los ingresos generados por concepto de impuestos, tasas y otros pagos relacionados con la propiedad, actividades comerciales, servicios municipales y otros aspectos regulados por la jurisdicción local.	Gerencia de Administración Tributaria, Desarrollo Económico y Turismo
SISTEMA INTEGRADO DE GESTION ADMINISTRATIVA -SIGA	Sistema de gestión pública centrándose en los procesos de abastecimiento y control patrimonial.	Todas las unidades orgánicas
SISTEMA INTEGRADO DE ADMINISTRACIÓN FINANCIERA - SIAF	Automatización de los procedimientos financieros para registrar los recursos públicos recaudados de la entidad.	Oficina General de Administración, Oficina de Contabilidad, Oficina de Tesorería, Oficina de Abastecimiento, Oficina de Recursos Humanos, Oficina de Tecnologías de la Información, Oficina General de Planeamiento, Presupuesto y Modernización e Inversión.
ZKTIMENET3.0	Gestiona las asistencias de los servidores públicos mediante el reloj marcador de la entidad.	Oficina de Recursos Humanos, Oficina de Tecnologías de la Información
SOFTWARE DE HISTORIAS CLINICAS ELECTRÓNICAS	Gestiona la información médica de los pacientes en formato digital.	Subgerencia de Salud y Bienestar Social
SISTEMA DE GESTION DOUMENTAL - SGD	Coordinar y controlar las actividades específicas que afecten a la creación, recepción, ubicación, acceso y preservación de la documentación.	Todas las unidades orgánicas
PAGINA INSTITUCIONAL	Plataforma digital diseñada para representar a una organización, proporcionando una ventana virtual que permite a los usuarios acceder a información relevante sobre la entidad.	Todas las unidades orgánicas

Municipalidad Distrital de La Punta OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

Municipalidad Distrital de La Punta OFICINA GENERAL DE ADMINISTRACIÓN OGA

7.2. Infraestructura de equipos de computo

EQUIPOS DE CÓMPUTO		
DESCRIPCIÓN	**CANTIDAD**	**AREA USUARIA**
Computadoras de escritorio	1	Alcaldía
	4	Procuraduría Pública Municipal
	5	Gerencia Municipal
	6	Órgano de Control Institucional
	15	Secretaria General, Archivo y Comunicaciones
	8	Oficina General de Administración
	4	Oficina General de Asesoría Jurídica
	7	Oficina General de Planeamiento, Presupuesto y Modernización e Inversión
	10	Gerencia de Desarrollo Urbano
	22	Gerencia de Desarrollo Humano
	18	Gerencia de Seguridad Ciudadana, Defensa civil y Policía Municipal
	7	Gerencia de Servicios a la Ciudad
	17	Gerencia de Administración Tributaria, Desarrollo Económico y Turismo
	14	Oficina de Abastecimiento
	16	Oficina de Tecnología de la Información
	10	Oficina de Tesorería
	10	Oficina de Recursos Humanos
	9	Oficina de Contabilidad

	7	Subgerencia de Gestión de Riesgo de Desastres y Defensa Civil
	24	Subgerencia de Salud y Bienestar Social
	6	Subgerencia de Gestión Ambiental
Laptop	4	Gerencia de Desarrollo Humano
	1	Gerencia de Desarrollo Urbano
	1	Gerencia Municipal
	1	Oficina de Contabilidad
	1	Oficina de Recursos Humanos
	5	Oficina de Tecnología de la Información
	1	Oficina General de Administración
	2	Oficina General de Planeamiento, Presupuesto y Modernización e Inversión
	5	Secretaria General, Archivo y Comunicaciones
	1	Subgerencia de Gestión de Riesgo de Desastres y Defensa Civil
Servidores	3	Oficina de Tecnología de la Información

7.3. Infraestructura de periféricos

EQUIPOS DE PERIFÉRICOS		
DESCRIPCIÓN	**CANTIDAD**	**AREA USUARIA**
Impresoras	2	Procuraduría Pública Municipal
	1	Gerencia Municipal
	3	Órgano de Control Institucional
	8	Secretaria General, Archivo y Comunicaciones
	2	Oficina General de Administración
	2	Oficina General de Asesoría Jurídica
	2	Oficina General de Planeamiento, Presupuesto y Modernización e Inversión
	4	Gerencia de Desarrollo Urbano
	7	Gerencia de Desarrollo Humano
	5	Gerencia de Seguridad Ciudadana, Defensa civil y Policía Municipal
	5	Gerencia de Servicios a la Ciudad
	7	Gerencia de Administración Tributaria, Desarrollo Económico y Turismo
	4	Oficina de Abastecimiento
	3	Oficina de Tecnología de la Información
	9	Oficina de Tesorería
	4	Oficina de Recursos Humanos
	1	Oficina de Contabilidad
	5	Subgerencia de Gestión de Riesgo de Desastres y Defensa Civil
	10	Subgerencia de Salud y Bienestar Social
	3	Subgerencia de Gestión Ambiental

7.4. Infraestructura de comunicaciones

EQUIPOS DE COMUNICACIONES	
DESCRIPCIÓN	**CANTIDAD**
Router	4
Switch	32
Acces Point	4
Torres de comunicación	3
Radios enlaces	4 pares

8. Identificación de riesgos

Los sistemas informáticos de la Municipalidad Distrital de La Punta están expuestos a una serie de riesgos que pueden comprometer la integridad, disponibilidad y confidencialidad de la información, así como la continuidad de las operaciones. A continuación, se detallan los principales riesgos identificados y sus respectivas descripciones e impactos:

a. Fallas de Hardware

Descripción: Posibilidad de fallas en componentes físicos esenciales, como servidores, discos duros, routers, impresoras y otros equipos debido a desgaste, sobrecarga, o problemas eléctricos.

Impacto: Puede ocasionar la pérdida parcial o total de datos críticos, interrupciones en los servicios y un tiempo de inactividad prolongado en las operaciones de la entidad.

b. Ataques Cibernéticos (Malware, Ransomware, Phishing, DDoS, etc.)

Descripción: Amenazas externas que buscan explotar vulnerabilidades en los sistemas de información mediante técnicas de hacking, infecciones de malware, suplantación de identidad o ataques de denegación de servicio.

Impacto: Puede resultar en la pérdida de datos sensibles, acceso no autorizado a la información, filtraciones de datos confidenciales o la interrupción de servicios críticos de la municipalidad.

c. Errores Humanos

Descripción: Errores o acciones inadecuadas de los usuarios y personal técnico, como configuraciones incorrectas, eliminación accidental de información, uso indebido de privilegios o descuidos en la seguridad.

Impacto: Puede derivar en la pérdida de datos, inestabilidad en los sistemas, fallos de seguridad o indisponibilidad del servicio.

d. Fallas de Software

Descripción: Errores en el software utilizado, como vulnerabilidades en el código, incompatibilidades entre sistemas, actualizaciones deficientes o configuraciones incorrectas de aplicaciones críticas.

Impacto: Podría ocasionar fallos en el funcionamiento del sistema, pérdida de información y aumento de vulnerabilidades en la seguridad del entorno informático.

e. Interrupciones del Suministro Eléctrico

Descripción: Cortes de energía eléctrica, picos de voltaje o fallos en la infraestructura eléctrica que afecten al Centro de Cómputo y otros equipos tecnológicos.

Impacto: Puede llevar a la pérdida de datos no guardados, daños en los equipos y la interrupción de los servicios de la municipalidad. La continuidad de las operaciones puede verse comprometida.

f. Desastres Naturales

Descripción: Eventos imprevistos como terremotos, inundaciones, incendios u otros desastres naturales que afecten las instalaciones o equipos tecnológicos.

Impacto: Riesgo de daño físico en los equipos, pérdida de datos críticos y paralización total o parcial de las operaciones en la municipalidad.

g. Infecciones por Malware o Virus

Descripción: Amenazas provenientes de software malicioso que pueden infectar y comprometer la integridad de los sistemas y datos.

Impacto: Pérdida de datos, robo de información confidencial, deterioro del rendimiento del sistema y daño a la infraestructura de red.

h. Interrupción de Servicios de Conectividad

Descripción: Fallos en el servicio de Internet, problemas con la red interna o fallos en los enlaces de comunicación que afecten la disponibilidad de los sistemas de información.

Impacto: Podría interrumpir la comunicación entre los usuarios y el servidor, limitar el acceso a aplicaciones en la nube y paralizar la operatividad de los procesos que dependen de la conectividad.

9. Plan de Acciones

9.1. Plan Preventivo

Está diseñado para evitar que se materialicen riesgos en los sistemas informáticos de la Municipalidad Distrital de La Punta mediante la implementación de medidas y prácticas que fortalezcan la seguridad desde la base. Se enfoca en la capacitación del personal, la actualización constante de los sistemas, el mantenimiento físico de los equipos y la adopción de procesos que minimicen la exposición a amenazas.

9.1.1. Capacitación Continua

Al formar continuamente al personal en buenas prácticas de seguridad, se reduce el riesgo de errores humanos, como el uso indebido de contraseñas o la apertura de correos electrónicos de phishing. Una fuerza laboral bien informada es menos susceptible a cometer acciones que puedan comprometer la seguridad de los sistemas. Por lo cual se realizara capacitaciones periódicas sobre buenas prácticas de seguridad informática, concientización sobre phishing, manejo seguro de datos y uso de herramientas de seguridad.

- Responsable: Oficina de Tecnologías de la Información.
- Frecuencia: Semestral.
- Evidencia: Registros de asistencia a capacitaciones y reportes de evaluación post capacitación.
- Reporte a: Oficina General de Administración.
- Cronograma:
    - Capacitación 1: Primera semana de junio.
    - Capacitación 2: Primera semana de diciembre.

9.1.2. Actualización de Sistemas

Mantener los sistemas operativos y software actualizados ayuda a cerrar vulnerabilidades que podrían ser explotadas por atacantes. Esto previene la entrada de malware o la explotación de fallos de seguridad conocidos, manteniendo así los sistemas protegidos contra amenazas emergentes. Por lo cual se actualizarán todos los sistemas operativos, aplicaciones y herramientas de seguridad para proteger contra vulnerabilidades conocidas.

- Responsable: Oficina de Tecnologías de la Información.
- Frecuencia: Mensual.
- Evidencia: Logs de actualizaciones o reportes generados manualmente.
- Reporte a: Oficina General de Administración.
- Cronograma:

- Actualización: Última semana de cada mes.

9.1.3. Gestión de Contraseñas

Regular el cambio de contraseñas es fundamental para minimizar el riesgo de accesos no autorizados a los sistemas informáticos. El uso de contraseñas robustas, con un nivel adecuado de longitud y complejidad, y su actualización periódica, complica los intentos de intrusión mediante ataques de fuerza bruta o técnicas de phishing. Por ello, se requerirá a los usuarios que actualicen sus contraseñas de manera periódica, cumpliendo con los requisitos establecidos en cuanto a longitud, complejidad y periodicidad.

De acuerdo con el punto 1.3 de la Directiva Nº010-2017-MDLP/OGA, "Directiva Administrativa para el Correcto Uso de los Equipos y Sistemas Informáticos de la Municipalidad Distrital de La Punta", donde se indica cómo elegir una contraseña, se establece que:

"La comunicación de las contraseñas se realizará de forma personal o vía teléfono, la misma que deberá ser cambiada inmediatamente por el usuario. Para elegir una contraseña, se recomienda lo siguiente:

a. Difícil de adivinar: Elegida aleatoriamente de un conjunto suficientemente grande como evitar la identificación como consecuencia de una búsqueda exhaustiva.
b. Secreta: Conocida solo por su dueño.
c. Tener al menos seis caracteres.
d. Tener una mezcla de letras, dígitos y/o signos de puntuación.
e. No coincidir con el número de cuenta o login, número de DNI, placa del automóvil o palabras escritas al revés.
f. Usar combinaciones de palabras cortas no relacionadas con uno o más signos de puntuación (rosa$vela, city%vidrio), palabras con dígitos insertados (avEN213ida, in80util), acrónimos (EulDlmdCnnQa), errores ortográficos (¿holgazán), consonantes y vocales alternadas en forma pronunciable pero sin sentido (bedugale, tuponsiga).
g. Evitar usar el mismo password para dos sistemas distintos."

- Responsable: Oficina de Tecnologías de la Información.
- Frecuencia: Semestral.
- Evidencia: Informes de cumplimiento de registros de cambios periódicos de contraseñas.
- Reporte a: Oficina General de Administración.
- Cronograma:
  - Cambio de contraseña: Segunda semana de junio y segunda semana de diciembre.

9.1.4. Respaldos Regulares

Realizar copias de seguridad de los datos es crucial para garantizar que, en caso de un fallo de hardware o un ataque como ransomware, la información crítica se pueda recuperar rápidamente, minimizando así la interrupción operativa. Por lo cual se realizará copias de seguridad regulares de todos los datos críticos y almacenarlas en lugares seguros, tanto localmente como en la nube.

- Responsable: Oficina de Tecnologías de la Información.
- Frecuencia: Semanal.
- Evidencia: Registros automáticos de respaldos, informes de verificación de integridad, y pruebas de recuperación de datos.
- Reporte a: Oficina General de Administración.
- Cronograma:
  - Respaldos completos: Cada domingo.
  - Verificación de integridad: Primer lunes de cada mes.

9.1.5. Mantenimiento preventivo de Equipos

El mantenimiento preventivo de los equipos informáticos es esencial para preservar su funcionamiento óptimo y prolongar su vida útil. Estas actividades reducen el riesgo de fallos críticos, garantizan la eficiencia de los sistemas y minimizan posibles interrupciones en el servicio.

De acuerdo con el procedimiento MDLP-UTI 018 de Mantenimiento Preventivo de Equipos de Cómputo, detallado en el Manual de Procedimientos (MAPRO) de la Oficina de Tecnologías de la Información, se han establecido las siguientes etapas para llevar a cabo un mantenimiento efectivo:

1. Instruir al equipo de Soporte Técnico la elaboración del Programa de Mantenimiento Preventivo a equipos de cómputo.
2. Elaborar el Programa de Mantenimiento y elevarlo al jefe para su aprobación.
3. Revisar el cronograma y verificar que estén considerados todos los equipos de la institución. En caso de haber observaciones, devolverlo para su modificación, regresando al paso 2.
4. Informar a la Oficina General de Administrativa (OGA) con el fin de comunicar a los usuarios la realización del Mantenimiento Preventivo de Equipos de Cómputo, adjuntando el cronograma.
5. Comunicar a los usuarios adjuntando el cronograma la realización del Mantenimiento Preventivo.
6. Los usuarios recibirán el documento con el cronograma en que se efectuará el mantenimiento preventivo de los equipos de cómputo.

7. Realizar el mantenimiento preventivo según el cronograma establecido.
8. Reinstalar los equipos y recabar firmas de conformidad en la Ficha de Mantenimiento Preventivo.
9. Firma de conformidad en la Ficha de Mantenimiento Preventivo por parte de los usuarios.
10. Recepción de la Ficha de Mantenimiento y su archivo en el expediente de Mantenimiento Preventivo de Equipos de Cómputo.

Este procedimiento asegura un enfoque sistemático para el mantenimiento de los equipos informáticos, garantizando su correcta operación y una adecuada gestión de la información y los servicios brindados por la municipalidad.

- Responsable: Oficina de Tecnologías de la Información.
- Frecuencia: Anual.
- Evidencia: Registros de mantenimiento de equipos.
- Reporte a: Oficina General de Administración.
- Cronograma:
  - Elaboración de Cronograma de Mantenimiento: Ultima semana de enero.
  - Ejecución del Cronograma: De febrero hasta diciembre.

Municipalidad Distrital de La Punta OFICINA DE TECNOLOGIAS DE LA INFORMACION

9.2. Plan Detectivo

Municipalidad Distrital de La Punta OFICINA GENERAL DE ADMINISTRACIÓN OGA

Se centra en la identificación temprana de amenazas y vulnerabilidades a través de la supervisión constante de los sistemas informáticos de la Municipalidad Distrital de La Punta. Incluye las herramientas que detecten actividades inusuales y la realización de auditorías que ayuden a descubrir posibles debilidades antes de que sean explotadas.

9.2.1. Monitoreo de Sistemas

Las herramientas de monitoreo permiten detectar comportamientos anómalos o accesos no autorizados en tiempo real. Al identificar estos riesgos de manera temprana, se pueden tomar medidas inmediatas para contenerlos y evitar que se propaguen o causen más daño.

Existen diversos sistemas de monitoreo que detecten actividades sospechosas o no autorizadas, con capacidad de generar reportes automáticos y que se utilizan para asegurar la integridad y el rendimiento de los sistemas informáticos en la Municipalidad Distrital de La Punta.

Entre ellos se incluyen:

Advanced Ip Scan: Escáner de red fiable y gratuito para analizar LAN. El programa escanea todos los dispositivos de red, le da acceso a las carpetas compartidas y a los servidores FTP.

Palo Alto Networks: Es un Firewall que clasifica el tráfico de red según la identidad de la aplicación y permite a los administradores controlar y visualizar todas las aplicaciones, incluidas las webs.

Consola de Administración Antivirus ESET NOD: Este software proporciona protección contra virus, malware y otras amenazas cibernéticas. Su función principal es detectar y neutralizar software malicioso, asegurando así la integridad de los datos y la seguridad de los sistemas.

Monitoreo de Red Zabbix: Es una herramienta de monitoreo de código abierto que permite supervisar el estado de la red, servidores y aplicaciones. Proporciona alertas en tiempo real y análisis de rendimiento, lo que ayuda a identificar y resolver problemas antes de que afecten a los usuarios finales.

- Responsable: Oficina de Tecnologías de la Información.
- Frecuencia: 24/7 continuo.
- Evidencia: Informes automáticos generados por las herramientas de monitoreo, logs de actividades sospechosas y reportes de incidentes detectados.
- Reporte a: Oficina General de Administración.
- Cronograma:
    - Revisión de logs y reportes: Diario, 08:00 AM.

9.2.2. Auditorías Periódicas

Las auditorías de seguridad revisan los sistemas en busca de vulnerabilidades no detectadas y evalúan la efectividad de las medidas de seguridad implementadas. Detectar debilidades a tiempo permite corregirlas antes de que sean explotadas por atacantes. Por lo cual se realizará auditorías de seguridad periódicas para identificar posibles vulnerabilidades en la infraestructura del sistema informático.

- Responsable: Oficina de Tecnologías de la Información.
- Frecuencia: Semestral.
- Evidencia: Informes de auditoría de seguridad.
- Reporte a: Oficina General de Administración.
- Cronograma:
    - Auditoría 1: Segunda semana de junio.
    - Auditoría 2: Segunda semana de diciembre.

9.2.3. Alertas y Notificaciones

Las alertas automáticas para incidentes críticos garantizan que el equipo de seguridad esté al tanto de los problemas tan pronto como ocurran, lo que permite una respuesta rápida y coordinada. Esto minimiza el tiempo en el que un sistema puede estar comprometido. Por lo cual se configurará alertas para incidentes críticos que requieran atención inmediata, estableciendo canales de comunicación claros para la respuesta rápida.

- Responsable: Oficina de Tecnologías de la Información.
- Frecuencia: 24/7 continuo.
- Evidencia: Registro de alertas y notificaciones enviadas.
- Reporte a: Oficina General de Administración.
- Cronograma:
    - Pruebas de funcionalidad: Primer viernes de cada mes.

9.3. Plan Correctivo

Tiene como objetivo restablecer la seguridad y funcionalidad de los sistemas informáticos de la Municipalidad Distrital de La Punta tras la identificación de un problema o incidente. Esto incluye la respuesta inmediata a los incidentes, el análisis detallado para entender la causa raíz, y la implementación de parches y soluciones para evitar futuras ocurrencias.

9.3.1. Respuesta a Incidentes

Contar con procedimientos claros y predefinidos para la respuesta a incidentes garantiza que cualquier amenaza o problema sea abordado de manera rápida y eficiente, minimizando los daños y restableciendo la operatividad de los sistemas en el menor tiempo posible.

Los incidentes contemplados están detallados en el punto 14 del Plan de Contingencia, y se describen a continuación:

a. Escenario I (Punto 14.1): Pérdida de comunicación entre los equipos de usuario y el servidor en la MDLP.
b. Escenario II (Punto 14.2): Falla de un servidor crítico.
c. Escenario III (Punto 14.3): Ausencia parcial o permanente del personal de la Oficina de Tecnología de la Información.
d. Escenario IV (Punto 14.4): Interrupción del suministro eléctrico.
e. Escenario V (Punto 14.5): Corte en el servicio de Internet.
f. Escenario VI (Punto 14.6): Indisponibilidad del Centro de Cómputo.

- Responsable: Oficina de Tecnologías de la Información.
- Frecuencia: Según necesidad.
- Evidencia: Informes de respuesta a incidentes que detallan las acciones tomadas, tiempo de respuesta y resultados obtenidos.
- Reporte a: Oficina General de Administración.
- Cronograma:
  - Simulacro de respuesta: Última semana de junio.

9.3.2. Análisis de Incidentes

Investigar y documentar los incidentes permite entender las causas raíz, lo que es esencial para prevenir que incidentes similares ocurran en el futuro. Este aprendizaje continuo fortalece la postura de seguridad de la organización.

- Responsable: Oficina de Tecnologías de la Información.
- Frecuencia: Según necesidad.
- Evidencia: Informes de análisis detallados que incluyan causas raíz, soluciones implementadas y medidas preventivas para evitar la recurrencia.
- Reporte a: Oficina General de Administración.
- Cronograma:
  - Informe semestral: Primera semana de enero y julio.

9.3.3. Parcheo y Actualización

Después de identificar una vulnerabilidad, aplicar parches y actualizaciones garantiza que el problema no persista. Esto es crucial para proteger los sistemas contra futuras amenazas que podrían explotar las mismas vulnerabilidades. Por lo cual se corregirá vulnerabilidades identificadas mediante la aplicación de parches y actualizaciones de software, priorizando las más críticas.

- Responsable: Oficina de Tecnologías de la Información
- Frecuencia: Según necesidad.
- Evidencia: Logs y reportes de parches aplicados, incluyendo detalles de vulnerabilidades corregidas.
- Reporte a: Oficina General de Administración.
- Cronograma:
  - Parches críticos: Dentro de las 24 horas de ser liberados.
  - Actualización general: Según necesidad.

10. Cronograma General de Actividades

Este cronograma general proporciona una visión clara de cuándo se llevarán a cabo las actividades clave para mantener la seguridad y el

funcionamiento óptimo de los sistemas informáticos en la Municipalidad Distrital de La Punta.

Actividad	Responsable	Fecha(s) Programada(s)
Capacitación Continua	OTI	Capacitación 1: Primera semana de junio. Capacitación 2: Primera semana de diciembre.
Actualización de Sistemas	OTI	Actualización: Última semana de cada mes
Gestión de Contraseñas	OTI	Cambio de contraseña: Segunda semana de junio y segunda semana de diciembre.
Respaldos Regulares	OTI	Respaldos completos: Cada domingo. Verificación de integridad: Primer lunes de cada mes.
Mantenimiento preventivo de Equipos	OTI	Elaboración de Cronograma de Mantenimiento: Ultima semana de enero. Ejecución del Cronograma: De febrero hasta diciembre.
Monitoreo de Sistemas	OTI	Revisión de logs y reportes: Diario, 08:00 AM.
Auditorías Periódicas	OTI	Auditoría 1: Segunda semana de junio. Auditoría 2: Segunda semana de diciembre.
Alertas y Notificaciones	OTI	Pruebas de funcionalidad: Primer viernes de cada mes.
Respuesta a Incidentes	OTI	Simulacro de respuesta: Última semana de junio.
Análisis de Incidentes	OTI	Informe semestral: Primera semana de enero y julio.
Parcheo y Actualización	OTI	Parches críticos: Dentro de las 24 horas de ser liberados. Actualización general: Según necesidad.

11. Costo del Plan y Fuentes de Financiamiento

El presente plan de seguridad para el mantenimiento de los sistemas informáticos de la Municipalidad Distrital de La Punta deberá considerar los costos asociados a las acciones preventivas, detectivas y correctivas detalladas anteriormente. Dichos costos incluyen las herramientas de monitoreo, recursos humanos entre otros. A continuación, se detallan los costos aproximados y sus respectivas fuentes de financiamiento:

DESCRIPCIÓN	2025	2026	2027	Fuente de Financiamiento
Licencias de Antivirus		31.000,00		Recursos Determinados
Almacenamiento en la Nube	2.000,00	2.000,00	2.000,00	Recursos Determinados
Mantenimiento preventivo de impresoras	15.000,00	15.000,00	15.000,00	Recursos Determinados
Mantenimiento preventivo de computadoras	20.000,00	20.000,00	20.000,00	Recursos Determinados
Mantenimiento preventivo del Data Center (servidores, switch, aire acondicionado)	35.000,00	35.000,00	35.000,00	Recursos Determinados
Mantenimiento de las torres de comunicación y radioenlace	40.000,00	40.000,00	40.000,00	Recursos Determinados
TOTAL	112.000,00	143.000,00	112.000,00	

Las fuentes de financiamiento previstas para la ejecución del presente plan incluyen el presupuesto asignado a la Oficina de Tecnologías de la Información (OTI) en el Cuadro Multianual de Necesidades para garantizar el éxito y la continuidad de este plan de seguridad.

12. Conclusiones

La implementación de este plan de seguridad es esencial para preservar la integridad, disponibilidad y funcionalidad de los sistemas informáticos de la Municipalidad Distrital de La Punta. A través de medidas preventivas, se busca reducir la probabilidad de incidentes, abordando posibles amenazas antes de que generen impactos significativos. Las acciones detectivas permiten una rápida identificación de amenazas o incidentes en tiempo real, lo que facilita una respuesta inmediata y minimiza el daño potencial a los sistemas. Finalmente, las acciones correctivas garantizan una recuperación eficiente y completa de los sistemas tras un incidente, solucionando las vulnerabilidades y previniendo su recurrencia. En conjunto, estas estrategias contribuyen a minimizar riesgos y asegurar la continuidad operativa de los servicios informáticos en la municipalidad, fortaleciendo la protección de los datos y procesos esenciales.

13. Recomendaciones

- Compromiso del Personal: Fomentar una cultura de seguridad informática en todos los niveles de la Municipalidad Distrital de La Punta. Esto incluye concientizar a cada miembro del personal sobre su papel en la protección de la información institucional y la prevención de riesgos informáticos.
- Revisión y Actualización Continua: Establecer un proceso regular de revisión y actualización del plan de seguridad, adaptándolo a nuevas amenazas y tecnologías emergentes. Este proceso debe incluir una evaluación de los sistemas y prácticas existentes, incorporando lecciones aprendidas y mejores prácticas de seguridad.
- Asignación de Recursos Suficientes: Asegurar la disponibilidad de recursos humanos, tecnológicos y financieros necesarios para la implementación efectiva de todas las medidas preventivas, detectivas y correctivas del plan. Esto incluye la capacitación continua del personal y la inversión en herramientas y tecnologías de seguridad.