"AÑO DE LA UNIDAD, LA PAZ Y EL DESARROLLO"

RESOLUCIÓN DE ALCALDÍA N°261-2023-A-MPM

Iquitos, 09 JUN 2023

VISTOS:

El Informe Legal N°396-2023-OAJ-MPM, de fecha 31 de mayo del 2023, y demás antecedentes; y;

CONSIDERANDO:

Que, el Artículo 194° de la Constitución Política del Perú, concordante con el articulo II del Título Preliminar de la Ley Orgánica de Municipalidades, Ley N°27972, establece que "las Municipalidades Provinciales y Distritales, son órganos de gobierno local que tienen autonomía política, económica y administrativa en los asuntos de su competencia; radicando esta autonomía en la facultad de ejercer actos de gobierno administrativo y de administración, con sujeción al ordenamiento jurídico";

Que, el artículo 197° de la Constitución Política del Perú, establece que las municipalidades promueven, apoyan y reglamentan la participación vecinal en el desarrollo local. Asimismo, brindan servicios de seguridad ciudadana, con la cooperación de la Policía Nacional del Perú, conforme a ley;

Que, el numeral 6) del artículo 20° de la Ley N° 27972 – Ley Orgánica de Municipalidades, establece que es atribución del Alcalde "Dictar Decretos y resoluciones de alcaldía, con sujeción a leyes y Ordenanzas";

Que, el artículo 59° del Reglamento de Organización y Funciones (ROF), aprobado con ordenanza N°005-2020-A-MPM, nos indica que, la Oficina de Sistemas y Tecnologías de la Información, es el órgano de apoyo de segundo nivel organizacional responsable de planificar, desarrollar, implementar y gestionar el gobierno electrónico, los sistemas de información, la infraestructura tecnológica y las telecomunicaciones que brindan soporte a las funciones desarrolladas por los diferentes órganos y unidades orgánicas de la Municipalidad Provincial de Maynas;

Que, el artículo 60° del Reglamento de Organización y Funciones (ROF), aprobado por ordenanza N°005-2020-A-MPM, nos indica que, son funciones específicas de la Oficina de Sistemas y Tecnologías de la Información (...) formular, elaborar y ejecutar un plan de contingencia de Seguridad Informática; desarrollar, implementar y mantener soluciones tecnológicas de seguridad a la información de la Municipalidad Provincial de Maynas, en el ámbito de sus competencias; (...);

Que, mediante Oficio N° 311-2023-OSTI-GM-MPM el Jefe de la Oficina de Sistemas y Tecnologías de la Información, remite al Gerente Municipal el "Plan de Formulación y Concientización en Seguridad TI", esto a razón de la recomendación de auditoría dada mediante Memorando (M) N° 054-2023-GM-MPM, que identificó la necesidad de elaborar un Plan de Formación y Concientización en Seguridad TI, la misma que permitirá fortalecer la capacidad tecnológica y la transformación digital;

Que, el Plan de Formación y Concientización en Seguridad TI, es dirigido a los usuarios de la Municipalidad Provincial de Maynas, con el fin de mejorar la gestión y

protección de los activos de información; asimismo, este plan aborda los principales desafíos en Seguridad TI, identificando los riesgos que pueden afectar a la organización y a los usuarios de ésta comuna edil, proponiendo una serie de actividades de formación y concientización para reducir la exposición de amenazas y mejorar la cultura de seguridad TI; asimismo, los objetivos del plan, están diseñados para mejorar la seguridad de la información en la comuna edil, y para reducir la exposición a las amenazas de seguridad TI;

Que, el Plan de Formación y Concientización en Seguridad TI, tiene establecidos los objetivos específicos, los grupos de usuarios que recibirán la formación, las áreas temáticas a tratar, los métodos y herramientas de formación, así como el calendario de formación y concientización;

Que, mediante el documento del Visto, la Oficina de Asesoría Jurídica, es de opinión que resulta procedente, aprobar el Plan de Formación y Concientización en Seguridad TI;

Que, estando a lo expuesto en el Artículo 43° de la Ley N°27972 - Ley Orgánica de Municipalidades, y contando con las visaciones de la Oficina de Asesoría Jurídica, Gerencia Municipal y la Oficina de Sistemas y Tecnologías de la Información;

SE RESUELVE:

ARTÍCULO PRIMERO: APROBAR el Plan de Formación y Concientización en Seguridad TI, presentado por la Oficina de Sistemas y Tecnologías de la Información de la Municipalidad Provincial de Maynas.

ARTÍCULO SEGUNDO: ENCARGAR, el cumplimiento de la presente Resolución a la Oficina de Sistemas y Tecnologías de la Información de la Municipalidad Provincial de Maynas.

ARTÍCULO TERCERO: ENCARGAR a la Oficina de Sistemas y Tecnologías de la Información, cumpla con publicar la presente resolución en el portal institucional de la entidad.

ARTÍCULO CUARTO: REMITIR, los actuados a Secretaría General de la Municipalidad Provincial de Maynas, a fin de que proceda conforme a sus atribuciones y para los fines que estime pertinente.

REGÍSTRESE, COMUNÍQUESE Y CÚMPLASE.

Econ. GERMAN VLADIMIR CHONG RIOS
ALCALDE

MUNICIPALIDAD PROVINCIAL DE

MAYNAS

Hagamos Historia

PLAN DE FORMACIÓN Y CONCIENTIZACIÓN EN SEGURIDAD TI

MUNICIPALIDAD PROVINCIAL DE MAYNAS

Descripción breve

Es un documento que tiene como objetivo establecer un plan de formación y concientización de los usuarios en temas de seguridad de la información en una organización. Este documento identifica los posibles riesgos en seguridad TI, establece objetivos específicos, define los métodos y herramientas de formación, crea un calendario de formación y concientización, y establece roles y responsabilidades para la implementación del plan. Además, incluye indicadores de éxito, actividades de evaluación y seguimiento, y recomendaciones para futuros planes de formación y concientización en seguridad TI. Este documento es esencial para proteger los sistemas de información de la organización y garantizar la seguridad y privacidad de la información confidencial.

OFICINA DE SISTEMAS Y TECNOLOGIAS DE LA INFORMACION

INDICE

I. Introducción

a) Descripción general del documento

La presente propuesta tiene como objetivo establecer un plan de formación y concientización en seguridad TI para los usuarios de la Municipalidad Provincial de Maynas, con el fin de mejorar la gestión y protección de los activos de información. Este documento está dirigido a los responsables de la seguridad de la información en la organización, con el objetivo de guiarlos en la implementación de una estrategia efectiva de formación y concientización en seguridad TI.

Este plan aborda los principales desafíos en seguridad TI, identificando los riesgos que pueden afectar a la organización y a los usuarios de la Municipalidad Provincial de Maynas, y propone una serie de actividades de formación y concientización para reducir la exposición a amenazas y mejorar la cultura de seguridad TI en la municipalidad.

El plan se basa en las mejores prácticas en seguridad TI y se enfoca en la capacitación y educación de los usuarios en el uso adecuado de los recursos de información, en la identificación de amenazas y en la adopción de buenas prácticas de seguridad TI. En este documento se establecen los objetivos específicos del plan, los grupos de usuarios que recibirán la formación, las áreas temáticas a tratar, los métodos y herramientas de formación, así como el calendario de formación y concientización.

La implementación del plan se llevará a cabo en estrecha colaboración con los responsables de la seguridad de la información y el personal de la Oficina de Sistemas y Tecnologías de la Información, quienes tendrán asignadas responsabilidades específicas para la ejecución de las actividades. Por último, se establecerá un proceso de evaluación y seguimiento para medir el éxito del plan y realizar los ajustes necesarios para su mejora continua.

b) Objetivos del plan de formación y concientización en seguridad TI

Los objetivos del plan de formación y concientización en seguridad TI son los siguientes:

- Sensibilizar a los usuarios de la Municipalidad Provincial de Maynas sobre la importancia de la seguridad de la información y su responsabilidad en la protección de los activos de información de la organización.
- Proporcionar a los usuarios de la Municipalidad Provincial de Maynas los conocimientos y habilidades necesarios para identificar y prevenir amenazas de seguridad TI, como virus, malware, phishing, entre otros.
- Fomentar la adopción de buenas prácticas de seguridad TI entre los usuarios de la Municipalidad Provincial de Maynas, como el uso de contraseñas seguras, la protección de los dispositivos móviles, la actualización de software y la realización de copias de seguridad de los datos.
- Aumentar la conciencia de los usuarios de la Municipalidad Provincial de Maynas sobre las políticas y normas de seguridad de la información de la organización, y la importancia de cumplirlas.
- Mejorar la cultura de seguridad TI en la municipalidad, promoviendo una actitud proactiva y responsable hacia la seguridad de la información.

Estos objetivos están diseñados para mejorar la seguridad de la información en la Municipalidad Provincial de Maynas, y para reducir la exposición a las amenazas de

seguridad TI. Al alcanzar estos objetivos, se espera que la municipalidad tenga una mayor confianza en la protección de sus activos de información, y que los usuarios de la Municipalidad Provincial de Maynas tengan una mayor conciencia y responsabilidad hacia la seguridad de la información.

II. Análisis de riesgos

a) Identificación de los posibles riesgos en seguridad TI

La identificación de los posibles riesgos en seguridad TI es una parte fundamental de este plan de formación y concientización. Se han identificado los siguientes riesgos en la Municipalidad Provincial de Maynas:

- **Acceso no autorizado a la red:** Los usuarios no autorizados pueden acceder a la red de la Municipalidad Provincial de Maynas, lo que puede resultar en la exposición no autorizada de datos sensibles.
- **Malware:** Los virus y otro malware pueden infectar los sistemas de la Municipalidad Provincial de Maynas, lo que puede resultar en la pérdida o corrupción de datos.
- **Ataques de phishing:** Los ataques de phishing pueden engañar a los usuarios para que proporcionen información confidencial, lo que puede resultar en el robo de datos.
- **Robo de dispositivos móviles:** Los dispositivos móviles de los usuarios de la Municipalidad Provincial de Maynas pueden ser robados, lo que puede resultar en la exposición de datos confidenciales.
- **Acceso no autorizado a los sistemas:** Los usuarios no autorizados pueden acceder a los sistemas de la Municipalidad Provincial de Maynas, lo que puede resultar en la exposición no autorizada de datos sensibles.
- **Incumplimiento de las políticas de seguridad:** Los usuarios pueden incumplir las políticas de seguridad establecidas, lo que puede resultar en la exposición de datos confidenciales.

La identificación de estos riesgos es fundamental para diseñar una estrategia de formación y concientización efectiva. Al identificar estos riesgos, se puede diseñar un programa de formación y concientización que aborde estos riesgos específicos y que proporcione a los usuarios las herramientas necesarias para mitigar estos riesgos. Además, se puede establecer un sistema de monitoreo y evaluación para garantizar que el programa de formación y concientización sea efectivo en la reducción de estos riesgos.

b) Evaluación de los riesgos identificados

Después de identificar los posibles riesgos en seguridad TI en la Municipalidad Provincial de Maynas se llevó a cabo una evaluación de los mismos. La evaluación se realizó para determinar la probabilidad y el impacto de cada riesgo identificado. A continuación, se presentan los resultados de la evaluación de riesgos:

- **Acceso no autorizado a la red:** Se considera que la probabilidad de este riesgo es moderada, ya que existen medidas de seguridad en la red para evitar el acceso no autorizado. Sin embargo, el impacto potencial de este riesgo es alto,

ya que la exposición de datos sensibles podría tener consecuencias graves para la municipalidad.

- **Malware**: La probabilidad de este riesgo se considera alta, ya que los virus y otro malware son comunes y pueden infectar los sistemas de la Municipalidad Provincial de Maynas. El impacto potencial de este riesgo es moderado, ya que la pérdida o corrupción de datos podría tener consecuencias graves, pero los sistemas de respaldo y recuperación de datos minimizan este riesgo.
- **Ataques de phishing**: La probabilidad de este riesgo se considera moderada, ya que los usuarios pueden ser engañados fácilmente por los ataques de phishing. El impacto potencial de este riesgo es alto, ya que el robo de datos sensibles puede tener consecuencias graves para la municipalidad.
- **Robo de dispositivos móviles**: La probabilidad de este riesgo se considera baja, ya que la Oficina de Sistemas y Tecnologías de la Información tiene medidas de seguridad física en su lugar para prevenir el robo. El impacto potencial de este riesgo es moderado, ya que la exposición de datos confidenciales podría tener consecuencias graves, pero los dispositivos móviles no contienen datos sensibles en la mayoría de los casos.
- **Acceso no autorizado a los sistemas**: La probabilidad de este riesgo se considera baja, ya que los sistemas tienen medidas de seguridad en su lugar para evitar el acceso no autorizado. El impacto potencial de este riesgo es alto, ya que la exposición de datos sensibles podría tener consecuencias graves para la municipalidad.
- **Incumplimiento de las políticas de seguridad**: La probabilidad de este riesgo se considera moderada, ya que los usuarios pueden olvidar o desconocer las políticas de seguridad. El impacto potencial de este riesgo es bajo, ya que el impacto de cualquier violación de la política de seguridad se minimiza mediante la formación y concienciación de los usuarios.

La evaluación de riesgos es importante para determinar qué riesgos son los más críticos y deben ser abordados con mayor urgencia en el plan de formación y concientización en seguridad TI. Con esta información, se puede desarrollar un enfoque de formación y concientización enfocado en abordar los riesgos más críticos y mejorar la seguridad general de la Municipalidad Provincial de Maynas.

c) **Priorización de los riesgos por su nivel de impacto y probabilidad**

Una vez identificados y evaluados los riesgos en seguridad TI en la Municipalidad Provincial de Maynas, se procedió a priorizarlos según su nivel de impacto y probabilidad. Para ello, se utilizó una matriz de riesgos, que permitió asignar una puntuación a cada riesgo en función de su impacto potencial y su probabilidad de ocurrencia.

Los riesgos identificados se clasificaron en cuatro categorías según su nivel de prioridad:

- **Riesgos críticos**: Aquellos riesgos que tienen una puntuación alta en la matriz de riesgos, es decir, un alto impacto potencial y una alta probabilidad de ocurrencia. Estos riesgos deben ser abordados de manera inmediata y prioritaria en el plan de formación y concientización en seguridad TI. En este caso, se identificó como un riesgo crítico el acceso no autorizado a la red.

- **Riesgos importantes:** Aquellos riesgos que tienen una puntuación media-alta en la matriz de riesgos, es decir, un impacto potencial moderado-alto y una probabilidad moderada-alta de ocurrencia. Estos riesgos deben ser abordados en el plan de formación y concientización en seguridad TI, pero pueden tener un plazo más amplio para su implementación. En este caso, se identificaron como riesgos importantes el malware y los ataques de phishing.
- **Riesgos menores:** Aquellos riesgos que tienen una puntuación media-baja en la matriz de riesgos, es decir, un impacto potencial bajo-moderado y una probabilidad baja-moderada de ocurrencia. Estos riesgos pueden ser abordados en el plan de formación y concientización en seguridad TI, pero pueden tener una menor prioridad. En este caso, se identificaron como riesgos menores el robo de dispositivos móviles y el acceso no autorizado a los sistemas.
- **Riesgos insignificantes:** Aquellos riesgos que tienen una puntuación baja en la matriz de riesgos, es decir, un impacto potencial bajo y una probabilidad baja de ocurrencia. Estos riesgos pueden ser ignorados o tratados con medidas generales de seguridad TI. En este caso, se identificó como un riesgo insignificante el incumplimiento de las políticas de seguridad.

La priorización de los riesgos por su nivel de impacto y probabilidad permite enfocar los recursos del plan de formación y concientización en seguridad TI en los riesgos más críticos y reducir el riesgo general de la Municipalidad Provincial de Maynas.

III. Plan de formación y concientización en seguridad TI

a) Objetivos específicos del plan de formación y concientización en seguridad TI

- Fortalecer la cultura de seguridad TI entre los usuarios de la Municipalidad Provincial de Maynas mediante la concientización y formación sobre buenas prácticas de seguridad.
- Reducir el riesgo de ataques cibernéticos mediante la capacitación del personal en la detección y prevención de amenazas como el phishing, el malware y los ataques de denegación de servicio.
- Proteger la privacidad y confidencialidad de los datos sensibles de la municipalidad a través de la capacitación en el manejo seguro de la información y en la gestión de contraseñas seguras.
- Reforzar las políticas y procedimientos de seguridad TI mediante la capacitación en la gestión de incidentes de seguridad, la identificación de vulnerabilidades y la implementación de medidas preventivas.
- Fomentar la responsabilidad individual en la seguridad TI mediante la capacitación en la identificación y reporte de incidentes de seguridad, así como la comprensión de las consecuencias legales y económicas de la violación de las políticas de seguridad TI.
- Aumentar la eficacia de la gestión de seguridad TI en la municipalidad a través de la capacitación del personal en el uso de herramientas de seguridad y en la comprensión de los roles y responsabilidades de cada miembro del equipo de seguridad TI.

Estos objetivos específicos permiten establecer metas concretas para el plan de formación y concientización en seguridad TI y enfocar los esfuerzos en áreas críticas para la seguridad TI de la Municipalidad Provincial de Maynas.

b) Identificación de los grupos de usuarios que recibirán la formación

- **Personal administrativo:** Incluyendo al personal que trabaja en las oficinas de contabilidad, recursos humanos, tesorería, entre otros. Estos usuarios manejan datos sensibles como información personal, financiera y de recursos humanos, por lo que requieren capacitación en el manejo seguro de información.
- **Personal técnico:** Incluyendo al personal encargado de la gestión de la infraestructura tecnológica, la implementación de medidas de seguridad y la administración de sistemas. Estos usuarios necesitan capacitación en la identificación y mitigación de vulnerabilidades y amenazas de seguridad.
- **Personal de atención al usuario:** Incluyendo a los encargados de brindar soporte técnico y atención al usuario. Estos usuarios necesitan capacitación en la detección y prevención de ataques de ingeniería social como el phishing y la suplantación de identidad.
- **Directivos y responsables de área:** Incluyendo a los jefes de departamento, coordinadores de proyectos, y otros responsables de áreas clave en la municipalidad. Estos usuarios necesitan capacitación en la gestión de incidentes de seguridad, en la implementación de políticas de seguridad TI y en la promoción de una cultura de seguridad TI dentro de sus equipos de trabajo.
- **Personal en general:** Incluyendo a todos los usuarios de la red y sistemas de la municipalidad. Estos usuarios necesitan capacitación básica en la seguridad TI, incluyendo el manejo de contraseñas seguras, la protección contra malware, la navegación segura en internet, entre otros.

La identificación de estos grupos de usuarios permitirá diseñar un plan de formación y concientización en seguridad TI que se adapte a las necesidades específicas de cada grupo, lo que contribuirá a la eficacia y eficiencia del programa de seguridad TI.

c) Descripción de las áreas temáticas a tratar en la formación

- **Políticas y normativas de seguridad TI:** Esta área temática se enfocaría en la comprensión de las políticas y normativas de seguridad TI que rigen en la municipalidad, incluyendo la Ley de Protección de Datos Personales, la Ley de Firma Electrónica y otros estándares de seguridad reconocidos internacionalmente.
- **Gestión de contraseñas seguras:** Esta área temática se enfocaría en la creación y manejo seguro de contraseñas, incluyendo la elección de contraseñas seguras, la utilización de gestores de contraseñas y las prácticas para compartir contraseñas seguras.
- **Amenazas y vulnerabilidades de seguridad TI:** Esta área temática se enfocaría en la identificación de amenazas y vulnerabilidades de seguridad TI, incluyendo el phishing, el malware, los ataques de denegación de servicio, las vulnerabilidades de software y otros riesgos.
- **Protección de la información:** Esta área temática se enfocaría en la protección de la información de la municipalidad, incluyendo la protección de los datos

personales, la gestión de la información confidencial, la protección de la información en tránsito y el almacenamiento seguro de información.

- **Uso seguro de dispositivos móviles**: Esta área temática se enfocaría en la gestión segura de dispositivos móviles, incluyendo la seguridad en el uso de smartphones y tablets, la protección contra el robo y pérdida de dispositivos y el uso de redes inalámbricas seguras.
- **Gestión de incidentes de seguridad**: Esta área temática se enfocaría en la gestión de incidentes de seguridad, incluyendo la detección, notificación y respuesta a incidentes de seguridad, así como el manejo de situaciones de emergencia.
- **Concientización y cultura de seguridad TI:** Esta área temática se enfocaría en la concientización y promoción de una cultura de seguridad TI en la municipalidad, incluyendo la promoción de buenas prácticas de seguridad, la identificación de los riesgos de seguridad y la comprensión de las consecuencias de la violación de las políticas de seguridad TI.

La descripción de estas áreas temáticas permitirá diseñar un plan de formación y concientización en seguridad TI completo y adaptado a las necesidades de la municipalidad. Además, esto contribuirá a la eficacia y eficiencia del programa de seguridad TI.

d) **Selección de los métodos y herramientas de formación**

- **Capacitaciones presenciales:** Estas capacitaciones pueden ser impartidas por expertos en seguridad TI y permiten la interacción directa entre los participantes y el formador. Las capacitaciones pueden incluir presentaciones, discusiones, estudios de casos y ejercicios prácticos.
- **Capacitaciones en línea:** Las capacitaciones en línea permiten la flexibilidad en cuanto a tiempo y lugar y pueden ser impartidas mediante plataformas de aprendizaje en línea. Estas capacitaciones pueden incluir videos, tutoriales interactivos, pruebas en línea y foros de discusión.
- **Simulaciones de ataques cibernéticos:** Estas simulaciones permiten a los participantes experimentar y aprender a detectar y responder a ataques cibernéticos en un ambiente seguro. Los participantes pueden aprender a identificar vulnerabilidades en el sistema, detectar intentos de phishing y malware, y aplicar las mejores prácticas de respuesta a incidentes de seguridad.
- **Talleres prácticos:** Los talleres prácticos pueden ser enfocados en la realización de ejercicios prácticos en los cuales se aprende a configurar, proteger y monitorear sistemas de seguridad TI en un ambiente controlado.
- **Videos educativos:** Los videos educativos son una forma sencilla y efectiva de transmitir información sobre temas de seguridad TI a un público amplio y diverso. Los videos pueden ser utilizados para ilustrar conceptos de seguridad, presentar casos de estudio y reforzar los conocimientos adquiridos en otras actividades de formación.
- **Boletines informativos:** Los boletines informativos son una forma efectiva de mantener actualizado a un público amplio y diverso sobre temas relevantes en seguridad TI. Los boletines pueden incluir noticias relevantes, actualizaciones de políticas y normativas de seguridad, consejos de seguridad y alertas de seguridad.

La selección de los métodos y herramientas de formación dependerá de los objetivos específicos del plan de formación y concientización en seguridad TI, la disponibilidad de recursos, y las necesidades y características de los grupos de usuarios que recibirán la formación.

e) Diseño de un calendario de formación y concientización

Mes	Actividad	Público objetivo	Método de formación
Enero	Introducción a la seguridad TI	Todos los usuarios	Capacitación presencial
Febrero	Protección de datos personales	Personal administrativo	Capacitación presencial
Marzo	Detección y prevención de phishing	Personal de TI	Capacitación presencial
Abril	Protección de redes y dispositivos móviles	Todos los usuarios	Capacitación presencial
Mayo	Políticas y normativas de seguridad TI	Gerentes y supervisores	Capacitación presencial
Junio	Gestión de contraseñas y autenticación	Personal de TI	Capacitación presencial
Julio	Seguridad en redes inalámbricas	Todos los usuarios	Capacitación presencial
Agosto	Monitoreo y detección de intrusos	Personal de TI	Capacitación presencial
Septiembre	Protección contra ransomware y malware	Todos los usuarios	Capacitación presencial
Octubre	Respuesta a incidentes de seguridad TI	Personal de TI	Capacitación presencial
Noviembre	Seguridad en aplicaciones web	Desarrolladores web	Capacitación presencial
Diciembre	Boletín informativo de seguridad TI	Todos los usuarios	Capacitación presencial

Este calendario tiene una duración de 12 meses y está diseñado para abarcar una amplia variedad de temas de seguridad TI relevantes para distintos grupos de usuarios. El método de formación utilizado en cada actividad está diseñado para maximizar la efectividad de la capacitación y la concientización en cada tema. Además, el calendario permite una distribución equilibrada de las actividades de formación a lo largo del año, lo que permite una mejor planificación y seguimiento.

IV. Implementación del plan de formación y concientización en seguridad TI

a) Descripción de los roles y responsabilidades de los actores involucrados en el plan

Rol	Responsabilidades
Responsable del plan	Este rol estará a cargo de la planificación, coordinación y supervisión del plan de formación y concientización en seguridad TI. Deberá asegurarse de que el plan se ajuste a los objetivos estratégicos de la municipalidad, asignar los recursos necesarios, y monitorear el progreso del plan para asegurarse de que se cumplan los plazos establecidos.
Equipo de capacitación y concientización	Este equipo se encargará de diseñar e implementar las actividades de formación y concientización en seguridad TI. Deberán tener conocimientos técnicos sólidos en seguridad informática, así como habilidades de enseñanza y comunicación efectiva para garantizar que los mensajes sean entendidos por todos los usuarios.
Gerentes y supervisores	Los gerentes y supervisores son responsables de garantizar que los empleados en sus áreas comprendan los riesgos de seguridad TI y de asegurar que sus equipos participen activamente en el plan de formación y concientización en seguridad TI.
Personal de TI	El personal de TI debe asegurarse de que la infraestructura de seguridad esté en su lugar y en buen estado, y de que se cumplan las normas y políticas de seguridad establecidas. Además, deberán participar en las actividades de formación y concientización para mantener sus habilidades actualizadas y compartir sus conocimientos con otros usuarios.
Usuarios	Todos los usuarios de la municipalidad son responsables de utilizar los recursos de TI de manera segura y de cumplir con las políticas y normativas de seguridad establecidas. Deben participar activamente en las actividades de formación y concientización y estar al tanto de las últimas amenazas de seguridad y las mejores prácticas de seguridad TI.

b) Planificación de las actividades a realizar en la implementación del plan

Actividad	Responsable(s)	Fecha de inicio	Fecha de finalización
Definición de objetivos específicos	Responsable del plan	10/09/2023	13/09/2023
Identificación de grupos de usuarios	Responsable del plan	14/09/2023	30/09/2023
Desarrollo del contenido temático	Equipo de capacitación y concientización	15/10/2023	30/10/2023
Selección de métodos y herramientas	Equipo de capacitación y concientización	01/11/2023	25/11/2023

Actividad	Responsable(s)	Fecha de inicio	Fecha de finalización
Diseño del calendario de formación	Responsable del plan	01/12/2023	14/12/2023
Implementación de las sesiones de formación	Equipo de capacitación y concientización	01/01/2024	31/12/2024
Evaluación de la efectividad del plan	Responsable del plan	01/12/2024	07/12/2024

c) **Identificación de los recursos necesarios para la implementación del plan**

Recurso	Descripción
Personal	Equipo de capacitación y concientización, responsable del plan, encargado de recursos humanos y jefes de áreas.
Tecnológicos	Equipos de cómputo, proyector, pizarra blanca, conexión a internet, plataforma de e-learning, software de seguridad y sistemas de gestión de aprendizaje.
Espacios	Salas de reuniones y aulas de capacitación.
Materiales	Papelería, folletos, manuales y material didáctico para las sesiones de formación.
Financieros	Presupuesto asignado para la implementación del plan, que incluye costos de personal, materiales, tecnología, transporte y otros gastos relacionados.

V. Evaluación y seguimiento del plan de formación y concientización en seguridad TI

a) **Definición de los indicadores de éxito del plan**

Indicador	Descripción
Número de usuarios capacitados	Número de usuarios que han completado el programa de capacitación en seguridad TI, desglosado por área y nivel de cargo.
Nivel de satisfacción de los usuarios	Porcentaje de usuarios que evalúan positivamente la calidad del programa de capacitación en seguridad TI en una encuesta de satisfacción realizada al finalizar la formación.
Reducción de incidentes de seguridad	Porcentaje de reducción de incidentes de seguridad después de la implementación del plan, medido en comparación con el periodo anterior a la formación, desglosado por tipo de incidente y departamento.

Indicador	Descripción
Cumplimiento de políticas de seguridad	Porcentaje de cumplimiento de las políticas de seguridad TI establecidas en la organización, medido antes y después de la implementación del plan.

b) Planificación de las actividades de evaluación y seguimiento del plan

Actividad	Descripción	Responsable	Frecuencia
Encuesta de satisfacción	Realizar una encuesta de satisfacción a los usuarios que han completado el programa de capacitación en seguridad TI para evaluar la calidad del programa y recopilar comentarios y sugerencias para futuras mejoras.	Equipo de capacitación y concientización	Al finalizar la capacitación
Evaluación de impacto	Realizar una evaluación de impacto del plan para medir el nivel de cumplimiento de los objetivos y evaluar la efectividad de las actividades de capacitación en la reducción de incidentes de seguridad y el cumplimiento de políticas.	Responsable del plan	Semestralmente
Auditoría de seguridad interna	Realizar una auditoría de seguridad interna para evaluar el nivel de cumplimiento de las políticas de seguridad establecidas en la organización y detectar áreas de mejora para la implementación de futuras iniciativas de seguridad.	Equipo de seguridad TI	Anualmente

c) Identificación de los ajustes necesarios para mejorar el plan

Ajustes necesarios	Descripción	Responsable
Actualización de contenidos	Identificar la necesidad de actualizar los contenidos de capacitación para incluir nuevas amenazas de seguridad, nuevas políticas de seguridad y cualquier cambio en las herramientas o tecnologías utilizadas en la municipalidad.	Equipo de capacitación y concientización
Ajustes en el calendario	Evaluar si el calendario de capacitación actual es adecuado para los usuarios y si se han realizado las sesiones de capacitación programadas en la fecha y hora establecidas.	Responsable del plan
Mejora en la implementación	Identificar cualquier problema o dificultad en la implementación del plan, como problemas técnicos o falta de	Equipo de capacitación y concientización

Ajustes necesarios	Descripción	Responsable
	compromiso de los usuarios, y tomar medidas para abordarlos y mejorar el proceso de implementación.	

VI. Conclusiones

a) Recomendaciones para futuros planes de formación y concientización en seguridad TI

- Realizar una evaluación de los riesgos en seguridad TI de manera regular para identificar nuevas amenazas y riesgos y así poder adaptar el plan de formación y concientización en consecuencia.
- Involucrar a la alta dirección en el diseño e implementación del plan, para lograr un compromiso y apoyo más efectivo en la asignación de recursos y presupuesto.
- Utilizar una variedad de herramientas y métodos de formación, para que los usuarios puedan aprender de diferentes maneras y se sientan más comprometidos con el proceso de aprendizaje.
- Realizar actividades de seguimiento y evaluación periódicas para medir el impacto del plan y hacer ajustes necesarios en consecuencia.
- Considerar la inclusión de actividades de concientización y formación para los contratistas y proveedores de servicios externos, ya que también pueden ser una fuente de vulnerabilidades y riesgos en la seguridad TI.

Estas recomendaciones podrían ser útiles para futuros planes de formación y concientización en seguridad TI, y ayudar a mejorar su efectividad e impacto en la seguridad de los sistemas de información.