



SECPLA
Secretaría Comunal de Planificación
Unidad de Informática

INFORME JUNIO 2025

DE : Alexis Antonio Alegría Riveros
Unidad de Informática
SECPLA

A : MIGUEL MUÑOZ VERDUGO
Secretario Comunal de Planificación

Padre Hurtado, junio del 2025

En función del cometido descrito en antecedente, señalado:

- **Crear materiales educativos adaptadas a las necesidades de los vecinos, incluyendo guías, manuales y tutoriales.**
- **Desarrollar campañas de sensibilización sobre ciberseguridad.**

A continuación, se presentan las acciones concretadas durante el periodo indicado, para las distintas iniciativas de inversión:

Se realizaron y compartieron nuevos comunicados por medio de correo electrónico con el fin de que los funcionarios se mantengan informados y adviertan a los vecinos de Padre Hurtado sobre los delitos cibernéticos más comunes (Anexo 1).

Se actualizaron campos en la Intranet destinada a los funcionarios municipales, donde podrán encontrar material relacionado al área tecnológica y el uso de algunas herramientas TIC de uso diario (Anexo 2).



SECPLA
Secretaría Comunal de Planificación
Unidad de Informática

ANEXOS

Anexo 1

INFORMATIV PRECAUCIONES ANTE CORREO MALICIOSO



Estimados funcionarios:

Se informa que se encuentra circulando un correo malicioso, el cual está diseñado con la intención de engañar, dañar, o robar información de los destinatarios. Estos correos suelen contener enlaces fraudulentos, archivos adjuntos infectados con malware o spyware, o mensajes que intentan suplantar la identidad de personas u organizaciones legítimas (phishing).

Lo que no se debe hacer	Lo que se debe hacer
<ul style="list-style-type: none">• No descargar ni abrir archivos adjuntos sospechosos o inesperados.• No hacer clic en enlaces incluidos en correos sospechosos.• No responder al correo proporcionando información personal, contraseñas, o datos confidenciales.	<ul style="list-style-type: none">• Informar al Departamento de Informática, quienes bloquearán dicho correo

Ejemplo de correo malicioso:

De: "ZimbraAdmin" <pausa@al.mil.gov.br>
Enviado: Martes, 20 de Mayo 2025 a las 15:58
Asunto: Actualización de cuenta #730212025

Estimado usuario,

Su cuenta ha sido comprometida. Nuestros registros indican que su cuenta **no se ha actualizado** como parte de nuestro mantenimiento regular y le recomendamos que siga las instrucciones del administrador a continuación para verificar su cuenta.

Nota: Su cuenta será suspendida si no la actualiza y verifica. Se recomienda que actualice su cuenta dentro de las 24 horas.

Haga clic en el enlace a continuación para actualizar su cuenta de correo web

actualización de cuenta

Proteger su cuenta es nuestra principal preocupación.

Atentamente,

Oficina de Servicios de Tecnologías de la Información

Este e-mail e quaisquer arquivos anexados são confidenciais e podem ser legalmente privilegiados. Se você não for o destinatário, qualquer divulgação, reprodução, cópia, distribuição ou outra disseminação ou uso desta comunicação é estritamente proibido. Se você recebeu esta transmissão por engano, por favor, notifique o remetente imediatamente e exclua este e-mail.

Não é possível garantir que a transmissão de e-mail seja segura ou livre de erros, pois as informações podem ser interrompidas, corrompidas, perdidas, destruídas, chegar atrasadas ou incompletas na conferência. O remetente, portanto, não aceita responsabilidade por quaisquer erros ou omissões no conteúdo desta mensagem que surjam como resultado de transmissão de e-mail ou alterações na data de transmissão não especificamente aprovadas pelo remetente.

Se este e-mail ou arquivos anexados contiverem informações que não estejam relacionadas à nossa atividade profissional, não nos responsabilizamos por tais informações.

Atentamente
Departamento de Informática

El Departamento de Informática está al tanto de este correo malicioso y ya ha implementado las medidas de seguridad necesarias para mitigar el impacto. Sin embargo, es posible que aún reciban correos similares durante los próximos días. Les pedimos que mantengan la calma, sigan las recomendaciones de seguridad y, ante cualquier duda, contacten de inmediato al Departamento de Informática al anexo 6038.

Más información
en:
intranet.mph.cl



SECPLA
Secretaría Comunal de Planificación
Unidad de Informática

INFORMATIV
PRECAUCIONES ANTE
LLAMADA MALICIOSA



Estimados funcionarios:

Hemos recibido reportes de llamadas sospechosas de parte de un supuesto "Magistrado", el cuál está solicitando un número de Whatsapp con el motivo de enviar y validar un "link". Esto corresponde a una llamada tipo Phishing, la cual tiene como motivo principal el hacer caer a los usuarios en un enlace con la finalidad de **robar datos personales**.

En el caso de recibir una llamada sospechosa, por favor seguir la siguientes recomendaciones:

Recomendaciones en caso de recibir una de estas llamadas	
No responder a llamadas de números desconocidos:	• Si recibes una llamada de un número que no reconoces, es mejor no contestar. Si contestas y la llamada parece sospechosa, cuelga inmediatamente.
No proporcionar información personal o financiera:	• Nunca compartas información sensible como números de tarjetas de crédito, contraseñas, o datos personales a través de llamadas telefónicas, especialmente si no reconoces al interlocutor. UN BANCO JAMÁS SOLICITARÁ CONTRASEÑAS.
Estar atento a las señales de alerta:	• Presta atención a llamadas que solicitan respuestas con "sí" o que ofrecen premios o beneficios inusuales. Estas pueden ser tácticas de estafa.
Verificar la identidad de quién llama:	• Si tienes dudas sobre la identidad de la persona que llama, puedes pedirle información de contacto y verificarla con la entidad que supuestamente representa.

En el caso de recibir estas llamadas, es importante mantener la calma, seguir las recomendaciones de seguridad y, ante cualquier duda, contactar de inmediato al Departamento de Informática al anexo 6038.

Atentamente
Departamento de Informática

Más información
en:
intranet.mph.cl

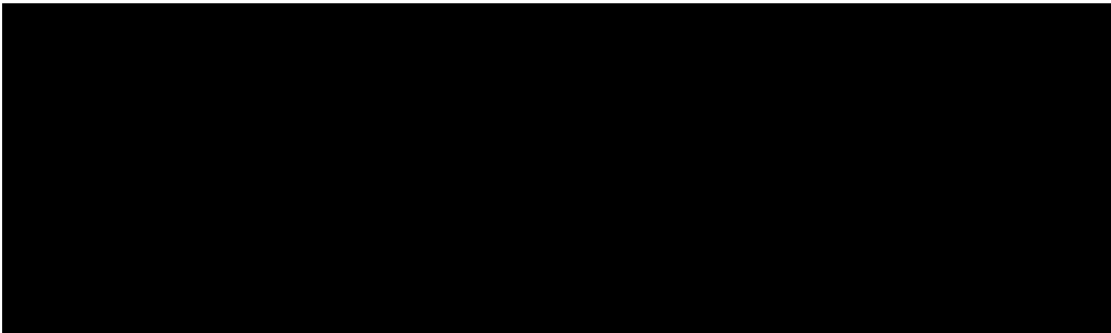


SECPLA
Secretaría Comunal de Planificación
Unidad de Informática

Informe de actividades realizadas durante año 2025

(Comprendido entre los meses de Enero a Junio)

Alexis Alegría Riveros





SECPLA

Secretaría Comunal de Planificación
Unidad de Informática

Durante el período comprendido entre los meses de Enero a Junio del 2025, se realizaron una serie de comunicados y actividades con el fin de cumplir los siguientes cometidos:

- **Crear materiales educativos adaptadas a las necesidades de los vecinos, incluyendo guías, manuales y tutoriales.**
- **Desarrollar campañas de sensibilización sobre ciberseguridad.**

Entre dichas actividades se encuentran:

- Envío de comunicados a los funcionarios por medio de correo electrónico con el fin de informar y advertir a los vecinos de Padre Hurtado sobre riesgos que podrían existir en el uso de internet y el cómo mitigarlos.

Entre los comunicados enviados se tocan los siguientes temas:

- o Consejos para usar el navegador de manera segura, entregando estrategias a los usuarios para que estos puedan tomar las medidas preventivas correspondientes al momento de navegar por internet.
- o Avisos y precauciones, así como los peligros que pueden representar los correos maliciosos (Spam, Phishing, etc.)
- o El uso seguro del celular y el computador.
- o Estafas informáticas comunes como lo son llamadas telefónicas y el cómo evitar caer en ellas.
- o Sobre la ingeniería social, en qué consiste y como aprender a identificarla.
- o Sobre la seguridad digital, tips para proteger los datos de usuario en las diferentes plataformas digitales.





SECPLA

Secretaría Comunal de Planificación

Unidad de Informática

INFORMATIVO

PRECAUCIONES ANTE CORREO MALICIOSO

Estimados funcionarios:

Se informa que se encuentra circulando un correo malicioso, el cual está diseñado con la intención de engañar, robar o sacar información de los destinatarios. Estos correos pueden contener enlaces fraudulentos, archivos adjuntos infectados con malware o spyware, o mensajes que intentan suplantar la identidad de personas u organizaciones legítimas (phishing).

Lo que no se debe hacer	Lo que se debe hacer
<ul style="list-style-type: none">No descargar ni abrir archivos adjuntos sospechosos o inesperados.No hacer clic en enlaces ocultos en correos sospechosos.No responder al correo proporcionando información personal, contraseñas, o datos confidenciales.	<ul style="list-style-type: none">Informar al Departamento de Informática, quienes investigarán dicho correo.

Ejemplo de correo malicioso:

De: "Miguel Ángel" <mi.angel@comunadepadrehurtado.cl>
Para: "Miguel Ángel" <mi.angel@comunadepadrehurtado.cl>
Asunto: Actualización de contraseña

Este es un correo electrónico malicioso que intenta robar información personal de los usuarios. Es crucial estar al tanto de las estrategias más comunes utilizadas por los atacantes para protegerse de estas amenazas.

En el caso de dudas o consultas, contactar con el Departamento de Informática al correo 6038 o a la Mesa de Ayuda al usuario 6000.

Más información en: intravet.mph.cl

El Departamento de Informática está al tanto de este correo malicioso y ya ha implementado las medidas de seguridad necesarias para mitigar el impacto. Sin embargo, es posible que aún reciban correos similares durante los próximos días. Los pedimos que mantengan la calma, sigan las recomendaciones de seguridad y, ante cualquier duda, contacten de inmediato al Departamento de Informática al correo 6038.

Más información en: intravet.mph.cl

INFORMATIVO

Riesgos de Correos Maliciosos

Estimados funcionarios:

Los correos electrónicos maliciosos, también conocidos como phishing, pueden adoptar diversas formas y emplear diferentes tácticas para obtener información confidencial de los usuarios. Es crucial estar al tanto de las estrategias más comunes utilizadas por los atacantes para protegerse de estas amenazas.

A continuación, se detallan algunos ejemplos de técnicas de phishing:

- "Actualización de correo electrónico": Este método engañoso solicita al usuario que ingrese sus credenciales de acceso para "confirmar" su cuenta.
- "Su cuenta ha sido bloqueada, ingrese sus datos para desbloquear": Esta técnica utiliza la urgencia para presionar al usuario a proporcionar sus credenciales de acceso al correo electrónico.
- "Su botón está sin espacio": Este tipo de mensaje induce al usuario a hacer clic en un enlace que lo lleva a una página falsa donde se le solicita ingresar sus credenciales de acceso.

¿Por qué es bueno esta información?

- Cada día surgen nuevas técnicas diseñadas para el robo de información y la realización de estafas. La importancia de estar informado sobre estos métodos es crucial, ya que permite mantenernos alerta ante la recepción de correos electrónicos maliciosos. Esta vigilancia no solo nos brinda la oportunidad de detectar un posible ataque, sino que también nos ayuda para advertir al resto del personal sobre la naturaleza engañosa de dichos correos.

Más información en: intravet.mph.cl

El Departamento de Informática jamás solicitará información personal como contraseñas o códigos de acceso.

En el caso de dudas o consultas, contactar con el Departamento de Informática al correo 6038 o a la Mesa de Ayuda al usuario 6000.

Más información en: intravet.mph.cl

INFORMATIVO

Riesgos de Correos Maliciosos

Estimados funcionarios:

Los correos electrónicos maliciosos, también conocidos como phishing, pueden adoptar diversas formas y emplear diferentes tácticas para obtener información confidencial de los usuarios. Es crucial estar al tanto de las estrategias más comunes utilizadas por los atacantes para protegerse de estas amenazas.

A continuación, se detallan algunos ejemplos de técnicas de phishing:

- "Actualización de correo electrónico": Este método engañoso solicita al usuario que ingrese sus credenciales de acceso para "confirmar" su cuenta.
- "Su cuenta ha sido bloqueada, ingrese sus datos para desbloquear": Esta técnica utiliza la urgencia para presionar al usuario a proporcionar sus credenciales de acceso al correo electrónico.
- "Su botón está sin espacio": Este tipo de mensaje induce al usuario a hacer clic en un enlace que lo lleva a una página falsa donde se le solicita ingresar sus credenciales de acceso.

¿Por qué es buena esta información?

- Cada día surgen nuevas técnicas diseñadas para el robo de información y la realización de estafas. La importancia de estar informado sobre estos métodos es crucial, ya que permite mantenernos alerta ante la recepción de correos electrónicos maliciosos. Esta vigilancia no solo nos brinda la oportunidad de detectar un posible ataque, sino que también nos ayuda para advertir al resto del personal sobre la naturaleza engañosa de dichos correos.

Más información en: intravet.mph.cl

El Departamento de Informática jamás solicitará información personal como contraseñas o códigos de acceso.

En el caso de dudas o consultas, contactar con el Departamento de Informática al correo 6038 o a la Mesa de Ayuda al usuario 6000.

Más información en: intravet.mph.cl

INFORMATIVO

Ciberseguridad en el celular

La ciberseguridad en el celular es la protección de los dispositivos móviles contra amenazas como el robo de información, el compromiso de cuentas, entre otros.

Consejos para proteger tu celular:

- Instala actualizaciones y parches de seguridad.
- Usa una contraseña fuerte o un sistema de identificación biométrica.
- Usa un VPN para cifrar tu conexión a Internet.
- Realiza copias de seguridad de tus datos.
- Evita abrir archivos adjuntos y enlaces sospechosos.
- Usa la aplicación de seguridad de tu dispositivo.
- Usa aplicaciones móviles (APP).
- Prefiere aplicaciones descargadas desde tiendas oficiales.
- Asegúrate de que la red WiFi sea segura.
- Bloquea tu dispositivo cuando no lo estés usando.

Más información en: intravet.mph.cl

El Departamento de Informática estará siempre disponible para responder consultas o dudas sobre el correcto uso de las tecnologías de la Información y Comunicaciones (TIC) con el fin de mitigar los riesgos de

Más información en: intravet.mph.cl



SECPLA

Secretaría Comunal de Planificación

Unidad de Informática

INFORMATIVO

Estafas telefónicas, llamadas grabaciones

Las llamadas telefónicas automáticas pregrabadas, o robocalls, son una forma de estafa que puede ser legal. Los estafadores pueden utilizar grabaciones de voz para cometer fraudes.

Cómo identificar una estafa telefónica por grabaciones:

- La llamada es automática y no es de una persona en vivo
- Se llamado intenta vender algo sin permitirte leer el número
- La llamada solicita información confidencial
- La llamada solicita pago de multas, la falta de regalo o giro
- La llamada solicita tarjetas de crédito para gastos de envío y manejo

Atentamente
Departamento de Informática

El Departamento de Informática estará siempre disponible para responder cualquier duda sobre el correcto uso de las tecnologías de la información y comunicaciones (TIC) con el fin de mitigar los riesgos de

Más información en: intranet.mph.cl

INFORMATIVO

INGENIERÍA SOCIAL: QUÉ ES

La Ingeniería social es un conjunto de técnicas de manipulación que utilizan los cibercriminales para obtener información confidencial de los usuarios, engañándolos para que revelen datos personales o financieros o para que realicen acciones perjudiciales.

Definición	La Ingeniería social es referida a los individuos que aprovechan la psicología humana para manipular a una persona y que resulta en acciones que no deseadas, como divulgar información sensible o revelar credenciales de acceso.
Objetivo	Los cibercriminales utilizan estas técnicas para obtener acceso no autorizado a sistemas, datos o información personal.
Ejemplos	Algunos ejemplos de ingeniería social para la explotación de identidad, el uso de identidad falsa para obtener la información para generar fraude o de confianza para permitir el acceso.
Profesión	Para protegerse de la ingeniería social, es importante ser conscientes de los fundamentos de la confianza, verificar la legitimidad de las solicitudes de información y no caer en técnicas manipulativas.
Caracteres	Los cibercriminales pueden utilizar diversos canales para hacer y recibir la ingeniería social, desde el correo electrónico, los mensajes de texto, los sitios web hasta el teléfono personal.
Según objetivos	Los cibercriminales pueden intentar persuadir los usuarios para que revelen información sensible o divulgan credenciales de acceso, comprometan sus dispositivos personales y sus identidades financieras o permitan instalar o ejecutar programas maliciosos, como spyware, para monitorear y controlar sus actividades, desde el momento de recibir a la víctima hasta el momento de su escape.
Prevención	Para prevenir la ingeniería social, es fundamental estar alerta, ser conscientes de los canales de comunicación, verificar la identidad de las solicitudes de información y no compartir información sensible con una desconocida persona.

Atentamente
Departamento de Informática

Más información en: intranet.mph.cl

INFORMATIVO

Ciberseguridad en el celular

La ciberseguridad en el celular es la protección de los dispositivos móviles contra amenazas como el robo de información, el intercambio de cuentas, entre otros.

Consejos para proteger el celular:

- Instalar actualizaciones y parches de seguridad.
- Usar una contraseña fuerte o un sistema de identificación biométrica.
- Usar una VPN para ofrecer tu conexión a internet.
- Realizar copias de seguridad de los datos.
- Evitar abrir archivos adjuntos y enlaces en correos electrónicos.
- Usar la aplicación de seguridad de tu dispositivo.
- Evitar aplicaciones, descargas desde fuentes no oficiales.
- Usar autenticación multifactor (2FA).
- Evitar aplicaciones, descargas desde fuentes no oficiales.
- Asignar de que la red WiFi sea segura.
- Bloquear el dispositivo cuando no lo estás usando.

Atentamente
Departamento de Informática

El Departamento de Informática estará siempre disponible para responder cualquier duda sobre el correcto uso de las tecnologías de la información y comunicaciones (TIC) con el fin de mitigar los riesgos de

Más información en: intranet.mph.cl

INFORMATIVO

MANUAL AVANZADO DE SEGURIDAD DIGITAL

En la era digital, la protección de nuestra identidad y datos personales se ha convertido en una necesidad imperante. Este manual profundiza en las mejores prácticas para la creación y gestión de contraseñas, así como en la implementación efectiva de la autenticación de dos factores, herramientas esenciales para salvaguardar nuestra información en el ciberespacio.

Clase Contraseñas Indefectibles	Al momento de crear una contraseña las recomendaciones que tenga una longitud de al menos 12 caracteres, incluir caracteres especiales (mayúsculas, minúsculas, números, símbolos) y evitar la información personal, además, se recomienda utilizar contraseñas memorables que sean únicas.
Autenticación de Dos Factores	Debe ser utilizada a una segunda forma de autenticación además de la contraseña, lo cual puede ser a través de códigos SMS, correo electrónico, etc. Para evitar el robo de contraseñas, se recomienda utilizar un dispositivo de protección en el caso de que la contraseña se vea comprometida.
Respuestas Seguras y Preguntas de Respuestas	Se recomienda responder a solicitudes de información y preguntas de seguridad con respuestas que incluyan palabras o frases personales que son desconocidas para otros usuarios.

La seguridad digital es un proceso continuo que requiere vigilancia y adaptaciones constantes. Al implementar las prácticas descritas en este manual, estás fortaleciendo significativamente tu defensa contra las amenazas cibernéticas.

Este documento detallado sirve como un recurso integral para **promover una cultura de seguridad digital** en nuestra comunidad. No complacémosnos a mantener este manual actualizado y a proporcionar apoyo continuo para garantizar la protección de nuestros recursos en el mundo digital.

Atentamente
Departamento de Informática

Más información en: intranet.mph.cl

INFORMATIVO

PRECAUCIONES ANTE CORREO MALICIOSO

El correo electrónico es una herramienta que se encuentra rodeado por un correo electrónico, el cual está diseñado con la intención de engañar, defraudar, o robar información de los destinatarios. Estos correos pueden contener enlaces fraudulentos, archivos adjuntos infectados con malware o spyware, o mensajes que intentan suplantar la identidad de personas o organizaciones legítimas (phishing).

Estados funcionales:

Se informa que se encuentra circulando un correo electrónico, el cual está diseñado con la intención de engañar, defraudar, o robar información de los destinatarios. Estos correos pueden contener enlaces fraudulentos, archivos adjuntos infectados con malware o spyware, o mensajes que intentan suplantar la identidad de personas o organizaciones legítimas (phishing).

Lo que NO se debe hacer:	Lo que SÍ se debe hacer:
<ul style="list-style-type: none"> • No dar lugar al clic en enlaces adjuntos sospechosos o inesperados. • No hacer clic en enlaces no habituales en correos sospechosos. 	<ul style="list-style-type: none"> • Informar al Departamento de Informática quienes bloquearon dichos correos.

No responder al correo proporcionando información personal, contraseñas, o datos confidenciales.

Ejemplo de correo malicioso:

Se recomienda reportar de inmediato a la Unidad de Informática cualquier correo sospechoso o inesperado.

Atentamente
Departamento de Informática

El Departamento de Informática está al tanto de este correo malicioso y ha implementado las medidas de seguridad necesarias para mitigar el impacto. Sin embargo, es posible que haya recibido correos similares durante los próximos días. Les pedimos que, si reciben recomendaciones de seguridad y, sobre todo, cualquier duda, contacten de inmediato al Departamento de Informática al correo it@secpla.cl.

Más información en: intranet.mph.cl

INFORMATIVO

PRECAUCIONES ANTE LLAMADA MALICIOSA

Se recomienda reportar de inmediato a la Unidad de Informática cualquier llamada sospechosa o inesperada.

Estados funcionales:

Se recomienda reportar de inmediato a la Unidad de Informática cualquier llamada sospechosa o inesperada.

En el caso de recibir una llamada sospechosa, por favor seguir las siguientes recomendaciones:

No responder a llamadas de números desconocidos	Evitar responder a llamadas de números desconocidos, especialmente si la llamada parece sospechosa o inesperada.
No proporcionar información personal o financiera	Nunca proporcionar información personal, financiera o sensible a través de llamadas de números desconocidos o sospechosos, especialmente si la llamada parece sospechosa o inesperada.
Evitar atender a las llamadas de phishing	Nunca atender a llamadas que soliciten información sensible, como contraseñas o datos personales, especialmente si la llamada parece sospechosa o inesperada.
Verificar la identidad de quién llama	Si tienes dudas sobre la identidad de la persona que llama, verifica la información de contacto y confirma con la entidad que te está llamando.

Atentamente
Departamento de Informática

Más información en: intranet.mph.cl





SECPLA
Secretaría Comunal de Planificación
Unidad de Informática

- Actualización de la Intranet Municipal según los comunicados enviados en el punto anterior, con el fin de que los funcionarios tengan material informativo para poder visualizar en cualquier momento y desde cualquier lugar en el caso de necesitarlos.

