SECPLA
Secretaría Comunal de Planificación
Unidad de Informática

INFORME JUNIO 2026

DE : **Alexis Antonio Alegría Riveros**
Unidad de Informática
SECPLA

A : **Miguel Muñoz Verdugo**
Secretario Comunal de Planificación

Padre Hurtado, junio del 2026
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 compartieron diferentes comunicados por medio de correo electrónico con el fin de que los funcionarios se mantengan informados e informen a los vecinos de Padre Hurtado sobre los delitos cibernéticos más comunes (Anexo 1).

Se habilitó un espacio en la Intranet destinada a los funcionarios municipales donde pueden 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

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 una 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 autenticación multifactor (2FA).
• Prefiere aplicaciones descargadas desde tiendas oficiales.
• Asegúrate de que la red WiFi sea segura.
• Bloquea tu dispositivo cuando no lo estés usando.

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

Atentamente
Departamento de Informática

Más información en:
intranet.mph.cl

INFORMATIVO

Tips para una navegación segura

Ten cuidado con los correos y enlaces	• Desconfía de correos electrónicos o mensajes con ofertas demasiado buenas para ser verdad. No hagas clic en enlaces sospechosos ni descargues archivos adjuntos de fuentes desconocidas (phishing).
Verifica los sitios web	• Asegúrate de que las URL de los sitios web comiencen con "https" (el candado en la barra de direcciones) y que la ortografía sea correcta.
Evita redes públicas	• No realices transacciones bancarias ni accedas a información sensible cuando uses redes Wi-Fi públicas. Si es necesario, usa una red privada virtual (VPN).
Cubre tu cámara web	• Cubre la cámara de tu computadora cuando no la estés usando para proteger tu privacidad física.

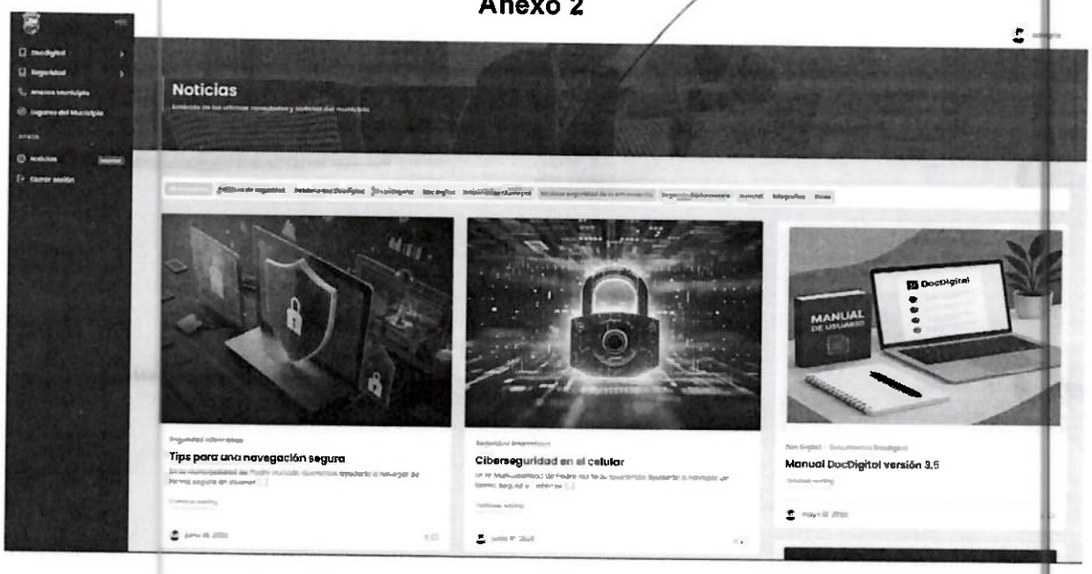
El **Departamento de Informática** estará siempre disponible para responder consultas o dudas sobre el correcto uso de las tecnologías de la información y comunicaciones (TIC) con el fin de mitigar los riesgos de

Atentamente
Departamento de Informática

Más información en:
intranet.mph.cl

SECPLA
Secretaría Comunal de Planificación
Unidad de Informática

Anexo 2



Sin otro particular, se despide atentamente,

[redacted]

SECPLA
Secretaría Comunal de Planificación
Unidad de Informática

Informe de actividades realizadas durante año 2026

(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 2026, 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:
  - 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.
  - Avisos y precauciones, así como los peligros que pueden representar los correos maliciosos (Spam, Phishing, etc.)
  - El uso seguro del celular y el computador.
  - Estafas informáticas comunes como lo son llamadas telefónicas y el cómo evitar caer en ellas.
  - Sobre la ingeniería social, en qué consiste y como aprender a identificarla.
  - Sobre la seguridad digital, tips para proteger los datos de usuario en las diferentes plataformas digitales.

MUNICIPALIDAD PADRE HURTADO
Somos Todos

SECPLA
Secretaría Comunal de Planificación
Unidad de Informática

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 una 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 autenticación multifactor (2FA). • Prefiere aplicaciones descargadas desde tiendas oficiales. • Asegúrate de que la red WiFi sea segura. • Bloquea tu dispositivo cuando no lo estés usando.

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

Atentamente
Departamento de Informática

Más información en: intranet.mph.cl

INFORMATIVO
Seguridad del correo electrónico

Consejos para un uso más seguro del correo electrónico

Lo que se debe hacer	Lo que NO se debe hacer
• Verificar el remitente del correo electrónico debido a posibles falsificaciones. • Verificar que el archivo adjunto no tenga doble extensión. (Por ejemplo: documento.doc.exe) • Verificar los dominios del remitente del correo electrónico antes de realizar cualquier acción (Ejemplo de dominio sospechoso: @[illegible]) • Reportar todos los correos electrónicos sospechosos al departamento de informática.	• No se debe abrir archivos adjuntos de correo electrónico que terminen con: .exe, .scr, .bat sin antes haber consultado al departamento de informática. • No se debe hacer clic en "cancelar suscripción" en cualquier correo electrónico de un sitio que no reconozcas, simplemente elimínalos y denúncialos. • No se debe hacer clic en una URL o link incrustada en un mensaje sospechoso o que no reconozcas. • No se debe responder a correos electrónicos sospechosos o no deseados, simplemente repórtalos con el área de informática y envíalos a la carpeta SPAM.

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

Atentamente
Departamento de Informática

Más información en intranet.mph.cl

INFORMATIVO
Informativo sobre el PHISHING

¿Qué es el PHISHING?

El phishing es una estafa digital donde ciberdelincuentes se hacen pasar por entidades confiables (bancos, empresas, conocidos) para engañar y robar información confidencial como contraseñas, datos bancarios o de tarjetas de crédito, usando correos electrónicos, SMS o llamadas falsas con enlaces a sitios web fraudulentos para capturar tus datos o instalar malware, todo con el fin de robar tu identidad y/o dinero.

¿Cómo funciona?	¿Cómo protegerte?
• El engaño: Recibes un mensaje que parece legítimo (ej. de tu banco) alertando de un problema urgente. • El señuelo: El mensaje incluye un enlace que te dirige a una página web falsa que imita a la real. • El robo: Al intentar "verificar" o "iniciar sesión" en esa página falsa, introduces tus datos, que son robados directamente por los atacantes.	• Desconfía de lo urgente: Ninguna empresa legítima te pedirá datos sensibles de forma inmediata por correo o mensaje. • Verifica la URL: Mira la dirección web (URL) del enlace antes de hacer clic; si no es el dominio oficial, no sigas. • No descargues adjuntos: Especialmente si no esperabas esos archivos. • Accede directo: Ve a la página de tu banco o servicio escribiendo tú mismo la dirección en el navegador, no desde un enlace. • Revisa el remitente: Busca errores o dominios extraños en la dirección de correo.

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

Más información en intranet.mph.cl

Atentamente
Departamento de Informática

INFORMATIVO
Informativo sobre el PHISHING

¿Qué es el PHISHING?

El phishing es una estafa digital donde ciberdelincuentes se hacen pasar por entidades confiables (bancos, empresas, conocidos) para engañar y robar información confidencial como contraseñas, datos bancarios o de tarjetas de crédito, usando correos electrónicos, SMS o llamadas falsas con enlaces a sitios web fraudulentos para capturar tus datos o instalar malware, todo con el fin de robar tu identidad y/o dinero.

¿Cómo funciona? / ¿Cómo protegerte? (misma tabla)

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

Más información en intranet.mph.cl

Atentamente
Departamento 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, dañar, o robar información de los destinatarios. Por lo cual, se llama a los usuarios a mantener la calma y no caer en este tipo de correos, ya que la información contenida es FALSA:

En el caso de recibir más correos de este estilo, por favor informar a Informática y enviar a la carpeta SPAM.

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.

Atentamente
Departamento de Informática

Más información en intranet.mph.cl

INFORMATIVO
CONSEJOS PARA USAR TU NAVEGADOR DE MANERA

Cuando el navegador te pida guardar contraseña, no aceptes	• [illegible]
Cierra las sesiones, no solo las ventanas	• [illegible]
Desmarca la opción de 'mantener la sesión abierta' al acceder a redes sociales o correo electrónico.	• [illegible]

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.

Atentamente
Departamento de Informática

Más información en: intranet.mph.cl

SECPLA
Secretaría Comunal de Planificación
Unidad de Informática

INFORMATIVO

CONSEJOS PARA USAR TU NAVEGADOR DE MANERA SEGURA 2

No instalar complementos de páginas desconocidas	• Si bien los complementos de los navegadores pueden facilitar el trabajo, algunos pueden contener intenciones maliciosas, por lo cual es importante instalar solo los ofrecidos por las páginas oficiales de su respectivo navegador.
Utilizar el modo "privado" en equipos compartidos o públicos	• Al utilizar el modo privado, el navegador no guardará historial, cookies o información ingresada en las páginas visitadas.
Evita páginas sospechosas o falsas	• Existen páginas maliciosas diseñadas para robar información, por lo cual se debe evitar acceder a páginas que tengan nombres extraños o sospechosos.

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: intranet.mph.cl

Atentamente
Departamento de Informática

INFORMATIVO

Informativo sobre el PHISHING

¿Qué es el PHISHING?

El phishing es una estafa digital donde ciberdelincuentes se hacen pasar por entidades confiables (bancos, empresas, conocidos) para engañar y robar información confidencial como contraseñas, datos bancarios o de tarjetas de crédito, usando correos electrónicos, SMS o llamadas falsas con enlaces a sitios web fraudulentos para capturar tus datos o instalar malware, todo con el fin de robar tu identidad y/o dinero.

¿Cómo funciona?	¿Cómo protegerte?
• El engaño: Recibes un mensaje que parece legítimo (ej. de tu banco) alertando de un problema urgente. • El señuelo: El mensaje incluye un enlace que te dirige a una página web falsa que imita a la real. • El robo: Al intentar "verificar" o "iniciar sesión" en esa página falsa, introduces tus datos, que son robados directamente por los atacantes.	• Desconfía de la urgencia: Ninguna empresa legítima te pedirá datos sensibles de forma inmediata por correo o mensaje. • Verifica la URL: Mira la dirección web (URL) del enlace antes de hacer clic; si no es el dominio oficial, no sigas. • No descargues adjuntos: Especialmente si no esperabas esos archivos. • Accede directo: Ve a la página de tu banco o servicio escribiendo tu mismo la dirección en el navegador, no desde un enlace. • Revisa el remitente: Busca errores o dominios extraños en la dirección de correo.

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

Más información en: intranet.mph.cl

Atentamente
Departamento de Informática

INFORMATIVO

Seguridad del correo electrónico

Consejos para un uso más seguro del correo electrónico

Lo que se debe hacer	Lo que NO se debe hacer
• Verificar el remitente del correo electrónico debido a posibles falsificaciones. • Verificar que el archivo adjunto no tenga doble extensión (Por ejemplo documento.doc.exe) • Verificar los dominios del remitente del correo electrónico antes de realizar cualquier acción (Ejemplo de dominio sospechoso: @gmail.org) • Reportar todos los correos electrónicos sospechosos al departamento de informática.	• No se debe abrir archivos adjuntos de correo electrónico que terminen con .exe, .scr, .bat sin antes haber consultado al departamento de informática. • No se debe hacer clic en "cancelar suscripción" en cualquier correo electrónico de un sitio que no reconozcas, simplemente elimínalos y denuncialos. • No se debe hacer clic en una URL o link incrustada en un mensaje sospechoso o que no reconozcas. • No se debe responder a correos electrónicos sospechosos o no deseados, simplemente reportalos con el área de informática y envíalos a la carpeta SPAM.

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

Más información en: intranet.mph.cl

Atentamente
Departamento de Informática

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". Este técnica utiliza la urgencia para presionar al usuario a proporcionar sus credenciales de acceso al correo electrónico.
- "Su buzón 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 necesaria esta información?
• Cada día surgen nuevas técnicas diseñadas para el robo de información y la realización de estafas. La importancia de estar informados 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 detener un posible ataque, sino que también nos capacita para advertir al resto del personal sobre la naturaleza engañosa de dichos correos.

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 anexo 6038 o a la Mesa de Ayuda al anexo 6000.

Más información en: intranet.mph.cl

Atentamente
Departamento de Informática

INFORMATIVO

Informativo sobre el PHISHING

¿Qué es el PHISHING?

El phishing es una estafa digital donde ciberdelincuentes se hacen pasar por entidades confiables (bancos, empresas, conocidos) para engañar y robar información confidencial como contraseñas, datos bancarios o de tarjetas de crédito, usando correos electrónicos, SMS o llamadas falsas con enlaces a sitios web fraudulentos para capturar tus datos o instalar malware, todo con el fin de robar tu identidad y/o dinero.

¿Cómo funciona?	¿Cómo protegerte?
• El engaño: Recibes un mensaje que parece legítimo (ej. de tu banco) alertando de un problema urgente • El señuelo: El mensaje incluye un enlace que te dirige a una página web falsa que imita a la real. • El robo: Al intentar "verificar" o "iniciar sesión" en esa página falsa, introduces tus datos, que son robados directamente por los atacantes.	• Desconfía de la urgencia: Ninguna empresa legítima te pedirá datos sensibles de forma inmediata por correo o mensaje • Verifica la URL: Mira la dirección web (URL) del enlace antes de hacer clic; si no es el dominio oficial, no sigas. • No descargues adjuntos: Especialmente si no esperabas esos archivos • Accede directo: Ve a la página de tu banco o servicio escribiendo tu mismo la dirección en el navegador, no desde un enlace • Revisa el remitente: Busca errores o dominios extraños en la dirección de correo.

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

Más información en: intranet.mph.cl

Atentamente
Departamento de Informática

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.

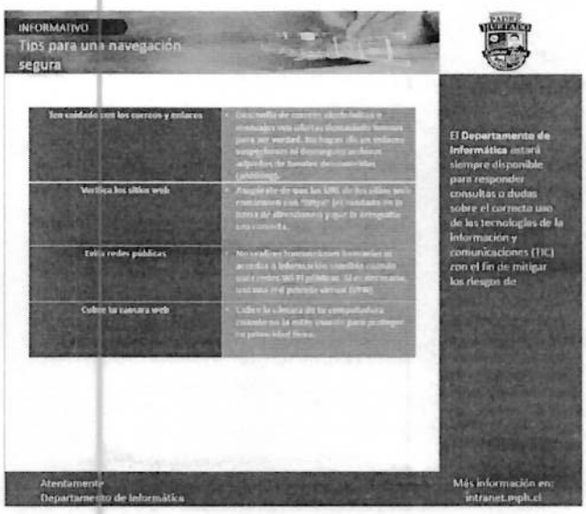
Consejos para proteger tu celular
• Instala actualizaciones y parches de seguridad. • Usa una contraseña fuerte o un sistema de identificación biométrica. • Usa una VPN para cifrar tu conexión a internet. • Realiza copias de seguridad de tus datos. • Evita abrir archivos adjuntos y enlaces sospechosos. • Usa la aplicación de seguridad de tu dispositivo. • Usa autenticación multifactor (2FA). • Prefiere aplicaciones descargadas desde tiendas oficiales. • Asegúrate de que la red WiFi sea segura. • Bloquea tu dispositivo cuando no lo estés usando.

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

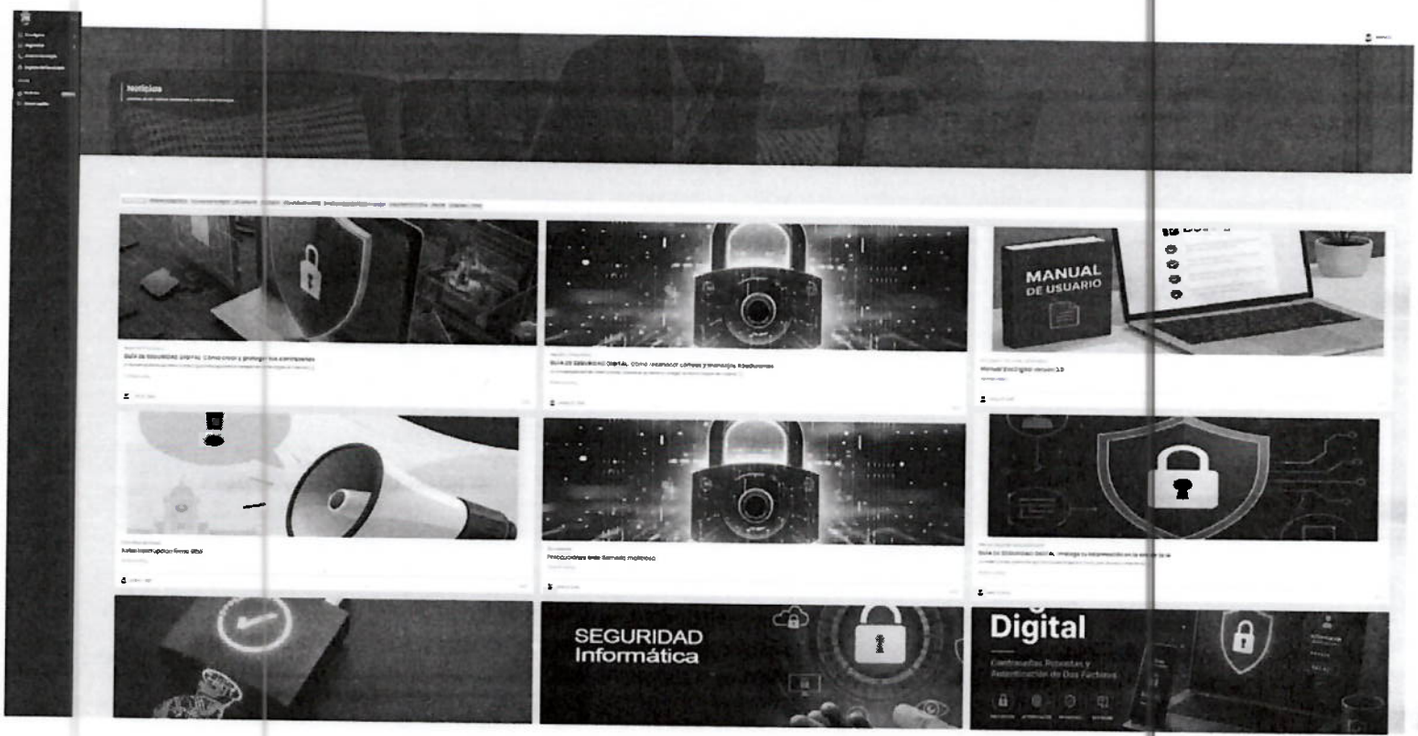
Más información en: intranet.mph.cl

Atentamente
Departamento de Informática

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.



[redacted]