Prácticas de Seguridad de Información - Comité de Seguridad MINSAL 2015

MANIPULACIÓN DE LA INFORMACIÓN

CONOCER LAS RESTRICCIONES AL TRATAMIENTO DE DATOS Y DE LA INFORMACIÓN SOLO PARA EL USO ESPECÍFICO AL QUE SE HA DESINADO.
POLÍTICA DE PROTECCIÓN DE DATOS Y PRIVACIDAD RES. EX. Nº 1082/2014

PROTEJA SU INFORMACIÓN

- ✓ Almacene la **información institucional SÓLO** en servidores, estaciones de trabajo o notebooks asignados por MINSAL.
- ✓ **NO** almacene **información personal** en estos equipos.
- ✓ Los equipos personales no son alternativa de almacenamiento de información de MINSAL.

PROTEGER LA INFORMACIÓN CONFIDENCIAL O CRÍTICA

- ✓ **NO copie** la información, salvo que exista autorización.
- ✓ **NO copie** la información que tenga prohibición por derecho de autor o licencia de uso.
- ✓ **Destruir** en forma segura (p.e. trituración).

ACUERDOS DE CONFIDENCIALIDAD

EN CONTRATOS, BASES O TÉRMINOS DE REFERENCIA

- ✓ Toda compra, contrato debe contener cláusulas necesarias para el resguardo de información de MINSAL.
- ✓ Debe contener cláusulas aludiendo al "Cumplimento lo establecido de las Políticas y Procedimientos de Seguridad de MINSAL, las que deben ser consultadas en **http://web.minsal.cl/seguridad_de_la_informacion.**

EN CONTRATOS DE RED

- ✓ Todo contrato de servicios de red, debe incluir características de seguridad y niveles de servicio.
  - Aplicación de tecnologías de autentificación, encriptación y control de conexiones
  - Reglas de acceso.

Prácticas de Seguridad de Información - Comité de Seguridad MINSAL 2015

ESCRITORIOS Y PANTALLAS LIMPIAS

REDUCIR LOS RIESGOS DE ACCESO NO AUTORIZADO, PÉRDIDA O DAÑO A LA INFORMACIÓN DURANTE Y FUERA DE HORAS NORMALES DE TRABAJO.

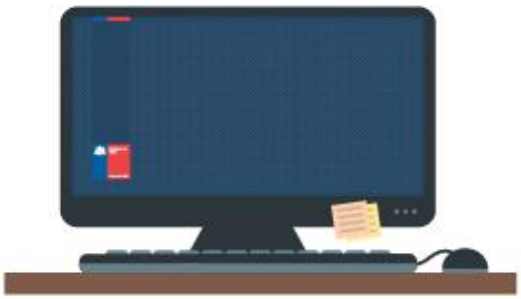
ESCRITORIOS LIMPIOS

Proteger la información confidencial en papeles y medios removibles

- ✓ **Guarde bajo llave** en gabinete o mobiliario seguro, cuando no se esté utilizando la información.
- ✓ Deje su lugar de trabajo en orden, **apague los equipos y guarde en un lugar seguro los documentos** al finalizar la jornada laboral.
- ✓ **No deje accesibles documentos** impresos que contengan datos confidenciales.
- ✓ **Retire los documentos de las impresoras** inmediatamente una vez impresos.

PANTALLAS LIMPIAS

Estaciones de trabajo y equipos portátiles protegidos



- ✓ **Cierre la sesión al ausentarse** o dejar de utilizar un sistema informático.
- ✓ Si debe abandonar, aunque sea momentáneamente, su puesto de trabajo, **bloquee su computador con un protector de pantalla** que solicite el ingreso de una contraseña.
  - Tecla Windows + L
  - Control + Alt + Supr

Respaldar nuestra información y protegernos de las descargas maliciosas de sitios web.

La seguridad de la información es un activo valioso en nuestra organización, debemos realizar nuestros respaldos de nuestra información, debemos tener cuidado con aquellos sitios web que contienen demasiada publicidad.

Cuidado con las descargas maliciosas.

Revisa la información de cada archivo a descargar, hay sitios que intentaran saturarte con botones o descargas que simulan lo que estas buscando.

Respalda tu información

Realiza respaldos periodicos de de la información con la que trabajas en el computador.

HOSPITAL DE LINARES

Ministerio de Salud

Gobierno de Chile

Prácticas de Seguridad de Información – Comité de Seguridad MINSAL 2015

USO DE CONTRASEÑAS

TODO ACCESO A LOS RECURSOS DE LA RED MINSAL DEBEN SER SOLICITADOS Y AUTORIZADOS POR EL DEPARTAMENTO DE GESTIÓN SECTORIAL TIC. REX EX. 1156/2014

NORMAS DE USO DE CLAVES

- ✓ Cuide que **nadie observe** cuando escribe su clave.
- ✓ **No escriba la clave** en papeles, post-it, ni en archivos sin cifrar.
- ✓ **No comparta su clave** con otra persona.
- ✓ **No pida la clave** de otra persona.
- ✓ **No habilite** la opción de "recordar claves" en los programas que utilice.
- ✓ **No envíe su clave por correo** electrónico ni la mencione en una conversación.
- ✓ **Cámbiela regularmente** o con la frecuencia establecida por la Unidad de Infraestructura TIC.
- ✓ Recuerde que los **intentos fallidos bloquean su cuenta** y los únicos encargados de desbloquear son Soporte TIC.

CREACIÓN DE CLAVES ROBUSTAS

- ✓ **No utilice** palabras comunes, de diccionario, ni nombres de fácil deducción por terceros, **no las vincule** a un dato personal.
- ✓ **No utilice** como contraseña su nombre de usuario ni derivados del mismo.
- ✓ Las contraseñas se deben construir utilizando como **mínimo 8 caracteres:**

  Donde debe incluir **al menos** una mayúscula, una minúscula y un número. Ejemplo: A23J77c31
- ✓ **Use claves distintas** para equipos y/o sistemas diferentes.
- ✓ Elija una **clave que no pueda olvidar**, para evitar escribirla en alguna parte.
- ✓ Toda **contraseña por omisión** provista por un fabricante o sistema **debe ser reemplazada.**

Ministerio de Salud

Gobierno de Chile

Prácticas de Seguridad de Información - Comité de Seguridad MINSAL 2015

USO DE INTERNET

LOS USUARIOS DEBEN UTILIZAR COMO 1ERA OPCIÓN PARA CONECTARSE A INTERNET LOS MEDIOS DISPUESTOS POR MINSAL. POLÍTICA PARA REGULAR EL USO Y NAVEGACIÓN DE INTERNET RES. EX. Nº 497/2013

NAVEGACIÓN SEGURA:

- ✓ Utilizar exclusivamente para **temas de trabajo.**
- ✓ Utilice un **navegador seguro** y con la configuración recomendada por la Unidad de Informática.
- ✓ **Evite acceder** a sitios desconocidos o no confiables.
- ✓ **No descargue** archivos de sitios web no confiables.
- ✓ **No debe aceptar** la instalación automática de software.
- ✓ **No ejecutar** archivos desde sitios dudosos.
- ✓ No hacer clic en el botón "ejecutar".

- ✓ **Tenga cuidado** con las conexiones WI-FI, no autorizadas por MINSAL:

  Las conexiones abiertas o sin contraseñas son peligrosas. Ajuste la configuración de su notebook o smartphone para evitar conectarse a redes desconocidas.
- ✓ Siempre descargue los archivos en una carpeta y **analícelos con un antivirus** actualizado antes de abrirlos.
- ✓ **No ingrese** información crítica o personal en formularios, páginas o foros.
- ✓ Sólo hágalo en **sitios seguros** (la dirección debe comenzar por **https**).
- ✓ **No almacene contraseñas** en los navegadores.

HOSPITAL DE LINARES

8 CONSEJOS PARA DETECTAR UN CORREO ELELECTRÓNICO FALSO.

No te fies del nombre, verifica la cuenta

Si por ejemplo recibes un correo del Hospital pero la cuenta que aparece es soporte1@hospitaldelinar.com en lugar de soporte@hospitaldelinares.cl fijate en la dirección de correo electrónico.

URLs fraudulentas

A veces el correo fraudulento te invita hacer clic en una URL engañosa. Antes de hacer clic verifica que el emisor pertenezca a tu libreta de direcciones, si tienes dudas puedes consultar con el Depto. TIC.

Falta de ortografía

Las empresas se toman la ortografía muy en serio. Un correo impecable denota seriedad y profesionalismo. Si encuentras faltas empieza a sospechar.

El mensaje te pide información personal

Activa las alarmas si un presunto correo de tu banco pide tu número de cuenta. El banco ya lo sabe al igual que tu contraseña.

No hagas clic en los adjuntos

Si un correo fraudulento tiene un archivo adjunto este incluirá malware que puede dañar tu sistema e incluso encriptar todos tus archivos. Hasta que no estes seguro de que el correo es fiable, no hagas clic en el adjunto.

Saludo estándar

Muchos correos legitimos de empresas emepezáran con un saludo personalizado que incluye tu nombre y tu apellido. Sospecha si un correo empieza con algo mas genérico como un “Estimado cliente”.

Ausencia de contactos

Lo normal es que un correo legítimo de una compañia termine con una firma que incluye diversos métodos de contacto. Si no hay ninguna forma de contactar con la empresa, es posible que te encuentres con un fraude.

Fiate de tu instinto

Es posible que la URL parezaca fiable, que no hallan faltas de ortografía. Pero si tienes la sensación que algo va mal, entonce confía en tu instinto. No pierdes nada con enviar un correo o llamar a la empresa para verificar la autenticidad del correo.