Buenas prácticas para usuarios

Contraseñas

- Las contraseñas son personales e intransferibles, no deben ser compartidas con otras personas, por ejemplo, compañeros de trabajo, familiares, subordinados o jefes.
- Utilizar contraseñas robustas para acceder a todos los servicios.
    - Elegir contraseñas de por lo menos 12 caracteres, preferentemente más de 14.
    - No utilizar nombres, fechas, palabras de diccionario, palabras con significado.
    - Incluir caracteres alfabéticos (letras mayúsculas y minúsculas), números, caracteres especiales.
- Utilizar reglas mnemotécnicas, para recordar mejor las contraseñas.
- Utilizar aplicaciones para registro seguro de contraseñas.
- Cambiar regularmente las contraseñas.
- Utilizar diferentes contraseñas para distintos servicios, diferenciar entorno laboral y entorno privado.
- Los mecanismos de doble factor de autenticación aportan un extra de seguridad, sobre todo en servicios críticos.
- Cambiar las contraseñas por defecto, no son seguras.

Entorno de trabajo

- Guardar sólo información pública en sitios de acceso público.
- Mantener el entorno de trabajo libre de documentación sensible.
- Mantener el software actualizado, aplicar los parches enviados por el proveedor de acuerdo con la política de seguridad de la información
- Utilizar programas anti-virus y anti-malware reconocidos y actualizados.

- Realizar copias de respaldo (backups) periódicos, actualizados y conservar en entornos distintos del de uso diario.
- Verificar la efectividad en la recuperación de la información, como se indica en la política de seguridad de la información.
- Dentro de lo posible utilizar software de VPN y conexiones seguras para acceder en forma remota a la información crítica.
- Verificar toda la información recibida fuera de los canales habituales para evitar tomar decisiones en base a información falsa.
- Evitar el uso de redes Wi-Fi libres y gratuitas, si no es posible, utilizar software de VPN
- Usar bloqueo automático de pantalla protegido con contraseña, para cuando no se encuentre el usuario en el puesto de trabajo.

Uso de correo electrónico

- Abrir los archivos adjuntos solo si fueron solicitados. Si los adjuntos vienen de un remitente conocido y no fueron solicitados, verificar la legitimidad de los mismos por un medio de comunicación diferente (comunicación telefónica, etc.) antes de abrir el adjunto.
- Verificar que el nombre del remitente coincide con la dirección de correo electrónico.
- Enviar correos con COPIA OCULTA, cuando se envíe información a distintas cuentas no relacionadas entre sí para evitar difundir direcciones de correo electrónico.
- Enviar información sensible en el texto del mensaje (claves, contraseñas, cuentas bancarias, tarjetas de crédito) sólo si está cifrada
- Verificar que el destinatario sea seguro antes de enviar imágenes de documentos o tarjetas.
- Descartar correos no deseados (SPAM) sin abrir.
- En caso de recibir solicitudes que no sean comunes, verificarlas por un medio de comunicación alternativo con el solicitante.

- Si recibe algún mensaje informando de la necesidad de cambiar contraseñas o acceder a cualquier sitio, verifique la veracidad del mensaje por un medio alternativo antes de acceder.
- Si recibe cualquier tipo de mensaje extorsivo o intimidatorio, comunicarlo inmediatamente al responsable de sistemas correspondiente.
- Desconfiar de los mensajes que informan sobre premios, herencias, donaciones, etc. ya que generalmente son el origen de estafas.

Navegación WEB

- No descargar software de fuentes no confiables.
- Atender los mensajes del navegador, acerca de sitios inseguros.
- Leer detenidamente la dirección URL de la página deseada, muchas veces los ciber-delincuentes cambian levemente una letra para impostar páginas seguras.
- No recordar usuario y contraseña si se utilizan equipos de acceso público.
- Siempre que se accede a una página con usuario y contraseña, salir cerrando la sesión.

Mensajería instantánea

- Rechazar contactos desconocidos.
- Ignorar archivos sospechosos o no solicitados.
- Transmitir información sensible sólo si la comunicación es cifrada de extremo a extremo
- Mantener actualizado el software de mensajería.
- Verificar por medio alternativo cualquier solicitud fuera de lo común.
- Resguardar los códigos de validación de acceso recibidos.
- Desconfiar cuando se recibe un llamado que genere sospecha o intimidación. No brindar información personal y verificar la comunicación por otro medio alternativo.

- Ignorar links recibidos del tipo “mira esto…”, aunque provengan de contactos conocidos.
- Verificar las fuentes de información, muchos ciber-delincuentes se presentan como representantes de instituciones reales, campañas de vacunación, instituciones bancarias, el propio empleador, etc.

Uso de PC compartidas

- Deshabilitar la función de autocompletar.
- Limpiar el historial y el cache del navegador. En lo posible utilizar navegación privada.
- Es preferible el uso de teclados en pantalla para ingresar contraseñas. Pero siempre evitar que terceros puedan ver mientras se ingresan las claves.
- Evitar realizar transacciones sensibles, como las bancarias, desde equipos de acceso público.

Redes sociales

- Evitar contactarse con desconocidos.
- Verificar cualquier información recibida.
- Revisar la configuración de privacidad.
- Configurar autenticación por doble factor.
- Mantener actualizada la información alternativa para el caso de recupero de cuentas y cambio de contraseñas.
- Limitar la información personal expuesta en el perfil de la cuenta. Verificar quién tiene acceso.
- Extremar los cuidados con la publicación de fotos, tanto por el contenido de la foto en sí, como otra información asociada que pueda obtenerse a partir de la misma.
- Limitar los permisos que se otorgan a las aplicaciones.