TÉRMINOS Y CONDICIONES DE USO

Importante: Lea atentamente este documento antes de utilizar la herramienta informática. No la utilice si no está de acuerdo con los Términos y Condiciones de este documento. El uso de la clave significa la conformidad con estos Términos y Condiciones de Uso. Usted está entrando a un Sistema Oficial perteneciente al Tribunal Electoral de la Provincia de Entre Ríos, el cual puede usarse solamente con fines autorizados. Solamente el personal designado para tal fin puede modificar las Páginas y Sistemas pertenecientes al dominio https://www.tribunalelectoraler.gob.ar. El uso de las claves gestionadas y proporcionadas sin la debida autorización puede resultar en una o varias penas de tipo criminal, civil o administrativo.

CONDICIONES DE USO

Toda persona, desde ahora "Usuario", que acceda y navegue por el dominio y/o utilice los correos electrónicos publicados en la web, deberá utilizar todos los elementos y medios puestos a su disposición en los sitios a los que acceda en un todo de acuerdo con las leyes, reglamentaciones y disposiciones gubernamentales vigentes y aplicables, así como con los presentes Términos y Condiciones de Uso, instructivos y demás avisos que sean publicados en https://www.tribunalelectoraler.gob.ar y que tengan como finalidad brindarle al Usuario orientación sobre la manera de proceder y utilizar los Sistemas y/o Servicios pertenecientes al Tribunal Electoral de la Provincia de Entre Ríos, entendiéndose por Servicios a toda la información proporcionada por el Tribunal Electoral de Entre Ríos o Terceros a través de su web, los Contenidos divulgados en soporte de papel y todos aquellos servicios que en el futuro pudiere ofrecer. Es por ello que el Usuario no deberá utilizar los Sistemas y/o Servicios con fines o efectos ilícitos; o que estuvieren prohibidos en los presentes Términos y Condiciones de Uso; o que pudieren dañar o menoscabar los derechos e intereses de terceros; o que de cualquier forma pudieren perjudicar o impedir la libre y normal utilización de los Servicios y/o Contenidos propios del dominio en cuestión, de Terceros, de otros Usuarios y/o de cualquier usuario de Internet. En este Documento, se hace mención a "Terceros", toda vez que personas físicas o jurídicas mediante la utilización de los Servicios brindados por el Tribunal Electoral de la Provincia de Entre Ríos hagan uso de los Contenidos a los que tuvieren acceso mediante la utilización del dominio https://www.tribunalelectoraler.gob.ar, refiriéndose como "Contenidos" a todo aquel documento digital de formato html, php, gif, jpg, bmp, pdf, xls, doc, y cualesquiera otro que sea utilizado para permitir el acceso a información, ya sea texto, imágenes, y todo otro tipo como el diseño gráfico y códigos fuente de los sitios pertenecientes al dominio tribunalelectoraler.gob.ar, que se encuentran protegidos por las leyes de derecho de autor reconocidas en los ámbitos nacional e internacional. En el supuesto de que un Usuario detectare, tuviere conocimiento o viere afectado sus derechos por el proceder incorrecto de otro Usuario en los sitios del dominio https://www.tribunalelectoraler.gob.ar, en violación de lo establecido por los presentes Términos y Condiciones de Uso, la moral y las buenas costumbres y la legislación aplicable, deberá notificar de inmediato a las autoridades correspondientes del Tribunal Electoral de la Provincia de Entre Ríos. Los sitios pertenecientes al dominio https://www.tribunalelectoraler.gob.ar puede incluir enlaces a otros sitios, los cuales se ofrecen como formas adicionales de acceso a la información allí contenida, entendiéndose como "enlace" o link a todo acceso hecho desde la citada web a otro sitio web y viceversa, ya sea html, php, no siendo esta enumeración taxativa y pudiendo extenderse a cualquier medio capaz de vincular contenido digital que posibilite cumplir las tareas para las que fuere habilitado el Usuario. El Tribunal Electoral de la Provincia de Entre Ríos no será responsable del contenido de ningún otro sitio o servicio que se ofrezca por medio de otros sitios. Si usted causa trastornos técnicos en este sitio o en los sistemas que transmiten este sitio a usted o a otros, usted admite su responsabilidad en todas y cada una de las penas civiles, criminales, o ambas, incluyendo pero no limitándose a daños y consecuencias que resulten del trastorno de los sitios, todo esfuerzo que se haga para corregir y restaurar el sitio.

El Tribunal Electoral de la Provincia de Entre Ríos se reserva el derecho, a su total discreción, de cambiar los términos, condiciones y restricciones de uso en cualquier momento poniendo en este sitio términos, condiciones y restricciones de uso revisados. Es responsabilidad del usuario chequear periódicamente para ver si el Tribunal Electoral de la Provincia de Entre Ríos ha hecho cambios a estos términos, condiciones y restricciones de uso. Continuar usando este sitio después de que en dicho sitio se han puesto cambios a estos términos, condiciones y restricciones de uso significa que usted acepta dichos cambios.

COMPROMISO DEL USUARIO

Es compromiso del Usuario que accede en forma autorizada a los sitios del dominio https://www.tribunalelectoraler.gob.ar del Tribunal Electoral de la Provincia de Entre Ríos, observar los siguientes ítems.

- Evitar ingresar datos falsos.
- Mantener la confidencialidad de la información reservada a la que eventualmente tuviera acceso en virtud de los permisos especiales otorgados por su condición de Usuario.
- Ingresar al sistema utilizando únicamente la identificación de Usuario y contraseñas asignadas por el Tribunal Electoral de la Provincia de Entre Ríos para tal efecto, y mantener esta última en estricta confidencialidad.
- Los usuarios no obtendrán acceso a los archivos de otros Usuarios o a los archivos del sistema sin la debida autorización.

La ausencia de controles de acceso no es una autorización para obtener acceso.
Obtener acceso sin la debida autorización, es una violación de las leyes y puede resultar en penas criminales o administrativas.
Los sistemas de información del Tribunal Electoral de la Provincia de Entre Ríos y los equipos relacionados están destinados a la comunicación, transmisión, procesamiento, y almacenamiento de información del Organismo. Estos sistemas y equipos están sujetos a monitoreo, protección contra el uso o acceso indebido y verificación de la presencia o funcionamiento de dispositivos o procedimientos de seguridad pertinentes. Tal monitoreo de seguridad puede resultar en la adquisición, registro y análisis de todos los datos que el usuario comunique, transmita, procese o almacene en este sistema. Si dicho monitoreo de seguridad revela evidencia de posible actividad criminal, tal evidencia podrá ser puesta a disposición del personal encargado de hacer cumplir las leyes. Usar este sistema constituye un consentimiento para dicho monitoreo de seguridad.
Se deberá notificar al Tribunal Electoral de la Provincia de Entre Ríos sobre cualquier situación o anormalidad detectada en el sitio que ponga en riesgo la integridad del mismo o la confidencialidad de los datos almacenados.
El Tribunal Electoral de la Provincia de Entre Ríos se reserva el derecho de dar de baja a usuarios que no cumplan estas condiciones y de filtrar electrónicamente las direcciones de Internet donde se sospechen actitudes maliciosas.
El usuario solo podrá utilizar la información entregada por el Servicio y/o Sistema al cual haya accedido desde cualquier sitio incluido en la web del Tribunal Electoral de la Provincia de Entre Ríos, para su uso en el ámbito que haya sido autorizado y no de forma personal o comercial y, en consecuencia, le queda prohibido ceder, comercializar, retransmitir o distribuir en cualquier forma y a cualquier título el todo o parte de dicha información.

RECOMENDACIONES PARA USO DE LOGIN Y CONTRASEÑA DE USUARIOS

Para efectos de autentificarse remotamente al Sistema, el Usuario contará con un identificador de usuario y una clave secreta o contraseña, que en su conjunto se denominará "**Clave Electoral**". Es obligación personal del Usuario que esta clave permanezca bajo su custodia y en la condición de secreta y de carácter intransferible. Evidentemente, uno de los problemas más comunes en seguridad informática no tiene que ver con malas implementaciones o problemas de ataques, sino que proviene de contraseñas inseguras o

fáciles de adivinar, lo cual es muy fácil de solucionar con sólo cambiar la contraseña. Lo que resulta realmente difícil es concientizar a los Usuarios para que utilicen contraseñas complejas. Por ello, no se debe usar una secuencia de dígitos y caracteres trivial en la formación de las clave secretas, cuando esta depende del Usuario. Existen numerosos ejemplos de claves que son descubiertas por simple deducción, por ejemplo el nombre, apellido, el nombre del hijo, el número de teléfono, número de documento, direcciones o claves otorgadas muy sencillas, por lo que debe ser cambiada por el Usuario al primer ingreso al Sistema.
Muchas vulnerabilidades están dadas por el descuido del propio Usuario. Algunas medidas básicas de protección incluyen el hecho de no anotar la contraseña en ningún lugar ni escribirla si alguien está observando. Es una norma tácita de buen Usuario no mirar el teclado mientras alguien teclea su contraseña. Se aconseja no enviar la misma por correo electrónico salvo la recibida oportunamente por el personal de Sistemas, ni mencionarla en una conversación. Se debe evitar mantener una contraseña indefinidamente por lo que se recomienda cambiarla en forma periódica. Hay que tener presente que la protección de la contraseña también recae en el Usuario dado que al comprometer una cuenta se puede estar comprometiendo todo el sistema. Para los Usuarios, muchas de las medidas de seguridad que se implementan son vistas como un contratiempo, como una exigencia sin consentimiento que lleva a cabo la gente de sistemas para justificar su trabajo y que no aporta ninguna ventaja; lo toman como una agresión o intromisión a su forma de trabajar y al final, y dentro de su lógica, terminan buscando la comodidad, como dejarlas anotadas para no ser olvidadas.
Hoy en día, existen herramientas específicas y automatizadas que pueden ser utilizadas para violar la seguridad de los sistemas informáticos recurriendo a ataques por fuerza bruta o ataques por diccionarios de contraseñas (wordlist) para intentar quebrarlas y así ingresar al sistema. Por ello siempre es recomendable limitar el tiempo de vida de las contraseñas evitando tenerlas el tiempo suficiente para que sean deducibles por cualquiera de los ataques mencionados. Absolutamente nadie, puede conocer su clave o pedir que cambie la suya a una conocida por él. Los procesos y sistemas están diseñados para operar sin que ningún colaborador deba saber su clave.

MEJORES PRÁCTICAS EN EL USO DEL CORREO DEL CORREO ELECTRONICO

Basado en las mejores prácticas para resguardar la información perteneciente al Organismo con respecto al uso de los recursos informáticos y teniendo en cuenta las implicancias respecto a la confidencialidad, la propiedad de la información transmitida en los mensajes, los códigos de ética y la privacidad del correo, se define a continuación cuál es la mejor forma de manejar el correo electrónico provisto al Organismo:

- Utilizar el correo electrónico como una herramienta de trabajo, y no como una casilla personal de mensajes a amigos y familiares.
- No enviar o reenviar archivos adjuntos dudosos, ya que podrían contener códigos maliciosos tales como virus, troyanos, gusanos, etc.
- Si se está trabajando con información del tipo confidencial, crítica o sensible, se deberán prever los mecanismos de seguridad necesarios previos al envío. Para ello y ante cualquier duda, se deberán consultar siempre las normativas internas impuestas para el caso, recordando que toda información tiene un propietario y no le corresponde al usuario decidir sobre el destino de la misma.
- Los correos no deben contener información que pudiera ser interpretada como ámbito de ataque, discriminación o ilegalidad. Todo lo que se escriba bajo el dominio del Organismo, es en representación del mismo, y las palabras podrían ser utilizadas de formas no previstas.
- Cuando se contesta un correo, hay que evitar poner "Responder a todos" a no ser que se esté absolutamente seguro que el mensaje debe ser recibido por "todos" los intervinientes.

RECOMENDACIONES PARA EVITAR SER VICTIMA DEL PHISHING

Esta información es brindada por la Oficina Nacional de Tecnologías de Información dependiente de la Subsecretaría de Tecnología y Ciberseguridad. Si recibe un correo electrónico que le pide información personal o financiera, no lo responda. Si el mensaje lo invita a acceder a un sitio web a través de un enlace incluido en su contenido, no lo haga. Las organizaciones que trabajan seriamente están al tanto de este tipo de fraudes y por consiguiente, no solicitan información por medio del correo electrónico. Tampoco lo contactan telefónicamente, ni mediante mensajes SMS o por fax. Si le preocupa el estado de la cuenta que posee en la organización que dice haber enviado el correo, o que lo ha contactado, comuníquese directamente utilizando un número telefónico conocido y provisto por la entidad u obtenido a través de medios confiables, como por ejemplo de su último resumen de cuenta. No envíe información personal usando mensajes de correo electrónico ya que éste, si no se utilizan técnicas de cifrado y/o firma digital, no es un medio seguro para enviar información personal o confidencial. No acceda al sitio web de una entidad financiera o de comercio electrónico desde computadoras instaladas en lugares públicos ya que estas podrían contener software o hardware malicioso destinado a capturar sus datos personales. Verifique los indicadores de seguridad del sitio web en el cuál ingresará información personal, escribiendo la dirección web usted mismo en el navegador y buscando los indicadores de seguridad del sitio. Al acceder al sitio web, usted deberá notar que la dirección web comienza con “https://”, donde la “s” indica que la transmisión de información es “segura”. Verifique también que en la parte inferior de su navegador aparezca un candado cerrado. Haciendo clic sobre ese candado, podrá comprobar la validez del certificado digital y obtener información sobre la identidad del sitio web al que está accediendo. No descargue ni abra archivos de fuentes no confiables, ya que estos archivos pueden tener virus o software malicioso que podrían permitir a un atacante acceder a su computadora y por lo tanto, a toda la información que almacene o introduzca en ésta. Si detecta o sospecha que ha sido víctima de un ataque de “phishing”, reenvíe el mensaje de correo electrónico y toda información que considere que puede ser de utilidad a: tribunalelectoral@entrerios.gov.ar