POLÍTICA DE CONTRASEÑAS & SEGURIDAD DE LA INFORMACION

Propósito

La presente política tiene como objetivo establecer los estándares de uso de claves y manejo de información de forma segura.

Las contraseñas son un aspecto muy importante de la Seguridad de la Información. Una contraseña débil puede dar lugar a accesos no autorizados y/o explotación de recursos de la empresa. Todos los usuarios con acceso a sistemas de la empresa son responsables de tomar las medidas adecuadas para seleccionar y proteger sus contraseñas.

Alcance

Esta política tiene como alcance establecer un estándar de uso de contraseñas seguras y su frecuencia de cambios. Esta política incluye a todo el personal que tiene o es responsable de una cuenta (de cualquier forma, de acceso que requiera una contraseña).

1.- Todas las contraseñas de usuarios deben ajustarse a las normas básicas de construcción y complejidad de las contraseñas.

2.- Las contraseñas deben tener un mínimo de 8 caracteres a un máximo de 10, en el cual se deben incluir letras Mayúsculas, Minúsculas, Números, Signos. EJ. L1t2mp$w3r

3.- No se pude utilizar la misma contraseña que tiene acceso a los sistemas de la compañía. Para otro tipo de acceso no relacionados con la empresa EJ: “Cuentas de correos personales, redes sociales, bancos, etc.”

4.- Las contraseñas tendrán una vigencia de 90 días. Los sistemas solicitaran de forma automática el cambio. Cabe mencionar que los sistemas no permitirán colocar claves utilizadas anteriormente.

5.- Las contraseñas no deben ser compartidas, estas deben ser tratadas como sensible.

6.- Se prohíbe escribir y guardas contraseñas en post-it o papel pegados en notebook o pantallas. Estas pueden ser vistas por otras personas colocando en riesgo su uso.

7.- No utilizar las funcionas de RECORDAR CONTRASEÑA de aplicaciones EJ: Navegadores “Chrome, Explorer”, Bancos, etc. Ya que todas las claves quedan guardadas en archivos ocultos dentro de Windows.

8.- Si el usuario ve o siente sospechas de que su contraseña fue vista o tomada ya sea porque le llego algún correo Phishing o encontró algún movimiento que no esta consciente de haber realizado. Se recomienda realizar de forma inmediata cambio de todas las contraseñas que utiliza como así también informar al departamento de tecnología.

9.- Siempre se debe validar los correos que se reciben. Ya que estos pueden venir de correos conocidos con archivos que no fueron solicitados. También validar el destinatario y empresa de donde viene el correo EJ: usuario@latampower.com este correo es correcto en el caso que venga usuario@latinpower.com el correo ya es extraño por lo que se tienen que tener cuidado al momento de abrir. También se debe tener en cuenta que citaciones y partes (Juzgados, SII, PDI, etc.” no son enviados por correo electrónico ya que son documentos sensibles y estos deben llegar por correo certificado.

10.- En el caso de tener dudas en el contenido del correo o destinatarios, se debe llamar al usuario que envió el correo y preguntar si el envío algún documento. Esto ayudara a que si la otra persona no envió el documento tome precauciones al respecto.

11.- Ante cualquier sospecha de virus, correo no deseado, o archivos ejecutándose de forma automática, se debe desconectar de la red el equipo “WIFI y LAN y llamar a departamento de tecnología. Cabe mencionar que uno de los fraudes mas comunes es el PHISHING. Este tipo de virus lo que hace es tomar la clave de correo y utilizar la cuenta solicitando información o bien dinero con deposito a cuentas extranjeras. El solo hecho de tomar nuestras credenciales. Las consecuencias pueden ser altas para la compañía.