Las 9 prácticas de empresas seguras.

- POR: WALTER URREA LEON.
  Ceo de Tecmanario. * Walter.Urrea@tecmanario.com

La constante transformación del trabajo producto del desarrollo exponencial de la tecnología, así como el auge y evolución de los ataques informáticos ha llevado a las organizaciones a adoptar nuevas formas no solo de desarrollar sus procesos de negocio sino de asegurarlos. Bajo este escenario y de la mano de profesionales expertos en tecnología, las empresas han implementado prácticas que involucran múltiples recursos.

Estas incluyen a todos y cada uno de sus colaboradores, independientemente del cargo que desempeñen; Tengan o no acceso a un computador, deben estar alineados con buenas prácticas en materia de seguridad.

Las prácticas mencionadas a continuación son producto de la experiencia y el consenso de muchos profesionales en tecnología que las han aplicado en múltiples organizaciones en los últimos años.

1. **Cuidar las contraseñas.**

   Hay un dicho que dice que las contraseñas son como la ropa interior: Personales, intransferibles y deben cambiarse con mucha regularidad. Es por esto que:

   - Las contraseñas se deben entregar formalmente a cada colaborador y acorde a las políticas de la compañía.
   - El detectar que un funcionario esta haciendo mal uso de sus contraseñas debe acarrear alguna sanción.
     Hoy en día es necesario habilitar en cada plataforma, el cambio obligado de la contraseña cada cierto tiempo.

2. **Administrar correctamente los perfiles.**

   Todo colaborador dentro de la organización tiene unas funciones asignadas conforme a un perfil del cargo, dicho perfil debe ser trasladado a su perfil informático. Es deber del administrador de la red es asignar y controlar los permisos de cada funcionario para evitar el acceso a recursos que no sean de su alcance y/o la manipulación de información que no es de su competencia.

3. Contar con seguridad perimetral.

Es necesario asegurar tanto el perímetro físico como el virtual. Desde un guarda de seguridad que evite el acceso no autorizado a nuestras instalaciones, pasando por un control de acceso mecánico o electrónico (molinetes, biometrico, tarjetas de próximidad etc), un software o suite de seguridad antivirus con reglas aplicadas para los equipos de usuarios y uno o varios dispositivos dedicados al control y monitoreo del tráfico de la red interna y las conexiones desde y hacia internet, correos, navegación etc. Todos resultan necesarios si de seguridad se trata.

4. Vigilar el uso de internet.

Hoy en día resulta más crítico que la empresa se quede sin acceso a internet a que pierda el acceso a un sistema como el contable por ejemplo. Por eso, es necesario vigilar que este recurso este bien utilizado por los usuarios. Una buena práctica es segmentarlo (crear VLans) asi no se mezclan usuarios con invitados y se aislan ciertos recursos críticos de aquellos que son de uso comun. La segmentación tambien permite asignar anchos de banda de conexión a internet por categoría o perfil, así como tambien priorizar el acceso de colaboradores y recursos que demanden mejor velocidad de conexión. Finalmente, restringir el acceso a sitios o servicios inoficiosos es otra práctica efectiva.

5. Mantener todo el software actualizado.

La última versión de todo software es el compendio de la depuración, el desarrollo, la experiencia, todo enfocado al mejoramiento del código fuente para que sea más estable, seguro, mejorar su rendimiento y así poder blindarlo de mejor forma contra ataques o fallos que puedan afectarlo.

Por regla, los administradores de tecnología siempre se mantienen una o hasta dos versiones atras, entre tanto se prueba y se estabiliza la nueva versión. Sin embargo, no es recomendable dejar pasar mucho tiempo antes de implementar la última versión lanzada. En especial cuando esta corrige fallos de seguridad de sus antecesoras. Y ni que hablar de los parches de seguridad o firmas como las utilizadas por antivirus; Estos deben permanecer actualizados siempre.

6. Supervisar el storage de la compañía.

Día a día generamos más y más información; Estructurada y no estructurada según los expertos en Big Data. Sin embargo es fundamental almacenarla adecuadamente, tanto a nivel local como remoto. Evitar al máximo la duplicación para óptimizar el almacenamiento. Controlar los medios externos como DVD, USB y demas es necesario para minimizar el riesgo de ingreso de malware a la

organización. Algunas compañias optan por restringir totalmente el uso de estos medios, otras los permiten con cierta cautela y solo para ciertos perfiles.

7. Generar más de un backup.

Actualmente es recomendable realizar tres backups:

a. Localmente: por la inmediatez de recuperar la información ante un desastre.
b. Remotamente. En caso de robo o daño del backup local o un eventual desastre natural debe existir otra copia en una ubicación geográfica alejada.
c. En internet. Los servicios cloud cada vez son mejores y la sobre-oferta ha logrado ampliar las modalidades de planes y disminuir los costos. Esta opción permite recuperar no solo la información sino tener un sistema completo operando nuevamente en pocos minutos, volviendo en el tiempo a una versión de pocas horas atrás.

8. Poseer autonomía eléctrica.

Todo lo anterior resulta insuficiente si no hay energia eléctrica suplementaria para evitar que se detengan los procesos en caso de falla del suministro eléctrico normal. Contar con equipos UPS y Planta generadora eléctrica que garanticen la autonomia energética por varias horas es necesario si la operación requiere continuidad.

9. Tener un plan de recuperación de desastres comprobado y actualizado.

Finalmente, el plan de recuperación de desastres involucra gran parte de las actividades mencionadas y busca poner a la organización en marcha nuevamente lo antes posible ante un desastre de cualquier tipo. El crearlo es apenas el primer paso, se debe probar frecuentemente y afinarlo conforme los resultados de las pruebas realizadas y los cambios que la organización vaya teniendo con el tiempo.