La importancia de la seguridad en la transformación digital

La oportunidad inobjetable que la transformación digital plantea para las empresas asume un comportamiento adecuado de sus colaboradores. Estos manejan datos, computadoras, redes, etc., y resulta que son seres humanos que, en su esfuerzo genuino por hacer bien las cosas pueden cometer errores o, en el peor de los casos, actuar intencionalmente mal para atacar al negocio. Es, por tanto, necesario que la empresa plantee ciertas políticas básicas que permitan discernir cuándo un incidente se debe a error humano y cuándo a un comportamiento doloso.

Las políticas de seguridad de la información deben promover tres grandes principios. El primer principio es la confidencialidad, en el sentido de “mantener los secretos en secreto”; información sensible sobre contratos, patentes, identificadores personales de tus clientes, entre otros, deben resguardarse para uso exclusivo interno. El segundo principio es el de disponibilidad, a fin de que los sistemas requeridos para operar en condiciones óptimas estén instalados correctamente, ganando así oportunidad. Por último, la política de seguridad de información debe promover la integridad, procurando precisión en las comunicaciones electrónicas (internas y corporativas), tales como: corroborar a quién se manda los correos electrónicos, revisando con cuidado los estados financieros y lo que declaran, etc.

Las políticas de seguridad de la información deben diseñarse con alcance a tres dominios. El primer dominio es el físico, que se refiere al perímetro físico de las oficinas en las que los colaboradores manipulan activos de información. El segundo dominio es el cibernético, que incluye la Internet, la nube, laptops, software y, en general, toda la tecnología en la que se desarrollan sus actividades. Por último, pero no menos importante, está el dominio humano, donde verificamos si las personas se están comportando de maneras extrañas o que puedan comprometer nuestra seguridad como empresas.

Los roles que cada uno de los colaboradores vive en su día a día también deben condicionar el tipo de políticas a implementar. Ciertamente, la mayoría de los empresarios visualiza fácilmente la vida profesional de sus colaboradores, en la que estos actúan para cumplir reglas, protocolos y políticas, tanto dentro de las instalaciones físicas del negocio como en trabajo a distancia (teletrabajo o “home office”). Sin embargo, cada uno de tus colaboradores tiene, aparte, una vida personal y otra móvil: los riesgos del dominio físico y hasta del cibernético pueden tocar incluso a las familias de los colaboradores, por lo que hay que considerar esto en las políticas para protegerlos; de manera similar, más allá de la oficina o del hogar, cada uno de tus colaboradores tiene conexión con otros a través de múltiples vías, por lo que debemos tomar medidas.

A continuación, te compartimos algunos consejos que debieran motivar el diseño e implementación de tus políticas de seguridad de información:

1. Al nomás identificar algo raro: todo colaborador debiera contactar a la persona indicada, para evitar riesgos.
2. Sobre contraseñas: nadie debiera escribirlas, ni usarlas más de una vez, ni hacerlas tan simples. El consejo más difundido al respecto es la aplicación del SNL: símbolos + números + letras (con mayúsculas y minúsculas). En general, debieran ser frases o grupos de palabras que tengan sentido para cada quien, fáciles para uno, pero difíciles para los demás: por ejemplo, una cita de un libro o de una película preferida. En este mundo digital, uno de los mayores miedos es el manejo de varias contraseñas; para suerte nuestra, existe ya software que permite administrar contraseñas personales con altos niveles de confiabilidad. Y lo más importante: nunca revelar tu contraseña a nadie.
3. Sobre software malicioso ("malware"): la creatividad de los enemigos del negocio se pone de manifiesto en diferentes tipos de software malicioso. Desde los famosos virus (que infectan y dañan los equipos), pasando por el "spyware" (que roba datos confidenciales en poder de la empresa), hasta llegar al "ransomware" (que te impide acceso a equipos y sistemas hasta que se pague un rescate), todos generan amenazas a la reputación del negocio y de su cadena de valor.
4. Sobre los "firewalls" humanos: toda tecnología, por avanzada que sea, requiere un apoyo decidido del equipo humano que la manipula para lograr su mayor provecho posible. Algunas costumbres sanas: verifica que toda página web que visites tenga https, ya que eso la vuelve más segura; siempre es buena idea cuidarse de dar demasiada información de identificación personal; al redactar mensajes de correo electrónico, fíjate bien si corresponde el botón "responder" o el "responder a todos", para evitar que gente no autorizada conozca información confidencial; cuidado con las redes sociales de cada colaborador (a quiénes se acepta como amigos y verificación de su identidad, publicaciones compartidas, políticas de internet en el trabajo).
5. Sobre la "ingeniería social": los estafadores suplantan identidades tratando de conseguir datos personales o bancarios, a través de llamadas telefónicas ("vishing") o de comunicación electrónica de algún tipo ("phishing"). Ante todo, conviene orientar a que los colaboradores usen el sentido común, pero también a la alta dirección a validar que ese sentido común exista. Entre los consejos al respecto, se pueden mencionar: triturar y destruir la basura de los contenedores, tanto en oficina como en casa; verificar la identidad de quien llama por teléfono y volver a llamarla después; tomar el tiempo de examinar mensajes, independiente del método de entrega.
6. Sobre movilidad y nube: el nuevo paradigma de trabajo nos lleva a usar más intensamente plataformas virtuales para almacenar y generar archivos digitales, así como conexión inalámbrica y aplicaciones móviles. Por lo mismo, las personas deben extremar sus medidas de prevención en todos los dominios de sus vidas. Algunos consejos valiosos: apague el bluetooth y el wi-fi mientras no los use; nunca uses redes públicas sin un VPN que cifre tu conexión y proteja tu información; establece políticas organizacionales que ayuden a prevenir, detectar y corregir riesgos y daños relacionados; protege tus móviles y laptops con

contraseñas; verifica las fuentes u orígenes de las aplicaciones (apps) que descargas a tus equipos.

7. Sobre copias de seguridad y mantenimiento: nada dura para siempre, ni la información digital. Por ello se debe siempre generar copias de seguridad y respaldos tanto en casa como en oficina.
8. Sobre el espacio de trabajo: el orden siempre será un mecanismo disuasivo del riesgo. Al levantarte siempre bloquea tu laptop, no olvides que cualquier cosa que se haga a través de ella será en tu nombre.
9. Sobre tarjetas de identificación y de acceso: las empresas van adoptando mecanismos de control de personal con tal de ordenarse y generar información valiosa para la toma de decisiones. Entre estos se encuentra el uso de tarjetas de identificación de los colaboradores, donde se consigna el nombre del mismo, códigos internos, ubicación organizacional y espacial, incluso imágenes; también se usa en algunos lugares tarjetas de acceso, que permiten que el personal autorizado acceda a ciertas áreas delicadas dentro de la operación y administración de la empresa. Si bien esto es muy bueno, también debe recordarse que estas pueden perderse o ser robadas mientras los colaboradores se trasladan fuera de las instalaciones del negocio, por lo que se debe extremar las medidas para su resguardo.

Evidentemente, las políticas no servirán de nada si nadie las cumple. En tal sentido, se hace necesario no solo diseñarlas, sino comunicarlas efectivamente a todo nivel dentro de la empresa, garantizando que cada colaborador sepa dónde encontrarlas cuando las necesite para consulta. De igual manera, es importante que cada colaborador sepa qué se espera exactamente de él respecto de dichas políticas, para evitar malentendidos. Finalmente, cada colaborador debiera ser responsable de establecer su propia política de seguridad en el hogar, para guardar alineamiento con el mundo de su trabajo.

Propemi BAC Credomatic pone a tu disposición la mejor plataforma de productos y servicios digitales y de banca móvil, que garantizan la seguridad de tus transacciones y movimientos bajo los más estrictos estándares. Sabemos el valor de cuidar a tus clientes, déjanos ayudarte a atenderlos como se merecen.