Published on *Revista .Seguridad* (https://revista.seguridad.unam.mx)


# CONCIENCIAR PARA PREVENIR

Edgar Ríos Clemente

awareness

numero-21

**¿CUÁNTOS DE NOSOTROS HACEMOS ACTIVIDADES DE PREVENCIÓN EN NUESTRO DÍA A DÍA? ¿CUÁNTAS DE ÉSTAS SON RELACIONADAS A NUESTRA SALUD? ¿Y A NUESTRA CIBERSEGURIDAD?**

De acuerdo al diccionario de la Real Academia Española, prevenir es la “preparación y disposición que se hace anticipadamente para evitar un riesgo o ejecutar algo”, también significa “anticiparse a un inconveniente, dificultad u objeción”.

Por lo que se refiere a prevención en la salud, uno debe preguntarse ¿Cuántos de nosotros vamos al doctor o al dentista de forma preventiva? Estoy seguro de que no somos unos cuantos los que nos esperamos hasta que ya no podemos soportar más algún dolor para hacer la visita obligada. Lo mismo sucede con los usuarios dentro de las organizaciones cuando hablamos de la prevención de riesgos de seguridad, ¿cuántos se acercan a sus áreas de seguridad de forma preventiva?, ¿a cuántos conoces que lleguen al área de soporte porque no tienen actualizada su firma de antivirus o en busca de las últimas actualizaciones de su sistema operativo? Todo esto no es más que el reflejo de la falta de cultura de prevención en nuestra sociedad.

Todavía hay muchas organizaciones que apenas están reaccionando ante los temas de seguridad, es decir, formando equipos de respuesta robustos o identificando servicios requeridos. Sin embargo, todas lidian con uno de los temas más difíciles de implementar en toda empresa, la administración de cambios organizacionales. Uno de estos es crear la costumbre de la prevención. Pero, ¿qué podemos hacer cada uno de nosotros para crear conciencia de los riesgos de seguridad de la información? Puedo decir que quienes saben de la importancia de la prevención, saben también las dificultades de implementarla.

Es importante resaltar que a la fecha se siguen presentando las mismas amenazas básicas de seguridad que desde hace más de una década. De acuerdo al reporte de la empresa Verizon, publicado en las noticias de seguridad de la CSI/UNAM-CERT el 23 de abril de 2014, es un hecho que los esfuerzos realizados no han sido suficientes y que deben crearse mejores programas de prevención.

Parece que las nuevas generaciones nacen con una habilidad asombrosa para operar cualquier dispositivo que se les ponga enfrente, por esto mismo, el tema de concienciación de la seguridad toma más relevancia, para que la prevención de riesgos en la seguridad sea un hábito.

Generar y promover iniciativas de prevención reducirá riesgos como fuga de información por ingeniería social, por citar un ejemplo. Está en cada uno de nosotros hacer los cambios necesarios para que los incidentes de seguridad no sean los mismos año tras año.

La concienciación para la prevención constituye un pilar importante para el cambio de la cultura organizacional en cuanto a temas de seguridad. Para que cumpla su objetivo, cada una de las actividades que propongamos en el marco de esta concienciación deberá estar dirigida a un sector específico, deberá contar con una serie de recomendaciones para su aplicación y de ser posible, estar relacionadas a la cotidianeidad de los usuarios. Trabajando la concienciación de este modo, será más fácil que unos padres puedan orientar a sus hijos dentro de sus hogares, por dar un ejemplo.

Crear conciencia de la importancia de la prevención y convertirla en un hábito nos beneficiará a todos. Pero si los esfuerzos no son bien dirigidos y la comunicación no es clara, se le restará atención a todo el proceso y el resultado podría ser adverso.

Concienciar para prevenir los riesgos de seguridad en ambientes digitales nos evitará muchos dolores de cabeza, incidentes en algunos casos, y explicaciones a la alta dirección.

Para crear una cultura proactiva en toda la población y en las organizaciones, se debe acelerar la disponibilidad de información, de recursos educativos y de concienciación, proporcionando las herramientas adecuadas para los usuarios.

Como un inicio básico, si eres un usuario casero debes proteger tu información y tus dispositivos electrónicos. Para hacerlo puedes encontrar información en el sitio de Usuario casero de la CSI/UNAM-CERT, en los sitios web de los mismos dispositivos o en las páginas de tus redes sociales, en éstas se indica qué hacer para configurarlos adecuadamente. En cuanto a recomendaciones de seguridad en servicios financieros, cada entidad tiene la obligación de proporcionarlas en sus páginas.

Si eres responsable de proporcionar servicios de seguridad, no olvides aprovechar las herramientas tecnológicas con las que tu organización cuenta en favor de la concienciación, como cursos de entrenamiento (internos y externos), bases de conocimiento, redes sociales (Twitter, Facebook, Instagram, Pinterest, entre otras), correo electrónico, herramientas de colaboración, posters, tableros de avisos, etc. Posteriormente deberás verificar que realmente se apliquen los cambios propuestos, es decir, revisar la eficacia de la campaña de concienciación mediante los incidentes de seguridad identificados. Puedes encontrar más información de cómo crear una campaña de entrenamiento en la publicación del National Institute of Standards and Technology NIST 800-50 “Building an Information Technology Security Awareness and Training Program” (Cómo construir una campaña de conciencia y entrenamiento para la cultura de seguridad).

La siguiente es una lista de recomendaciones básicas de prevención por la que debemos iniciar:

## UTILIZAR CONTRASEÑAS SEGURAS

Utiliza diferentes combinaciones para usuarios y contraseñas y evita escribirlas. Recurre a frases

fáciles de recordar o nombres de canciones, puedes utilizar la primera letra de cada palabra combinándolas con caracteres especiales.

## EN LA COMPUTADORA Y DISPOSITIVOS MÓVILES

Mantén actualizado el sistema operativo y las aplicaciones, de preferencia activa la opción de actualizaciones automáticas. Utiliza un antivirus/antimalware y configúralo para que realice las actualizaciones automáticas.

## PROTEGE TU IDENTIDAD DIGITAL




Se precavido al proporcionar información personal en medios digitales. Verifica que los sitios que visitas sean seguros y habilita configuraciones de privacidad.

## EN LOS MEDIOS SOCIALES

Asegúrate de que la configuración de tu perfil sea en su mayoría privada y ten cuidado con la información que publicas.

## PROTEGE TUS DISPOSITIVOS MÓVILES

Recuerda que también pueden ser blancos de *malware* y de usuarios malintencionados. Para protegerte habilita la contraseña de acceso y descarga aplicaciones sólo de sitios de confianza.

## ASEGURA TU RED INALÁMBRICA

Las redes inalámbricas, si no son configuradas adecuadamente, pueden ser vulnerables, sobre todo las redes públicas, debes evitar realizar transacciones financieras en estas redes.

## EVITA NAVEGAR EN SITIOS Y ARCHIVOS DESCONOCIDOS

Si no has solicitado esa información, evita abrir los mensajes desconocidos que te llegan.

## SOLICITA LA AYUDA CORRECTA

Cuando eres víctima o sospechas de un incidente de seguridad, contacta al equipo de atención a incidentes de seguridad de tu organización o solicita servicios profesionales, la UNAM cuenta con el UNAM-CERT.

Si requieres apoyo en la instalación de aplicaciones, consulta a tus proveedores o contacta a un técnico profesional.

**Si quieres saber más consulta:**

- Usuario casero
- Comic Liga Super-Seg
- Noticias SSI-UNAM
- 2014 Data Breach Investigations Report
- NIST Special Publication 800-50 - Building an Information technology Security Awareness and training Program
- NIST Bulletin - Information Technology Security Awareness, Training, Education, and Certification

---