Enero, 2021

BOLETÍN INFORMATIVO DE CIBERSEGURIDAD

Mecanismos Preventivos en la Seguridad Informática

Nivel de Importancia: ALTA (4)

¡Lo que deberíamos saber!!!

Todas las personas y en especial las empresas públicas y privadas, que almacenan información muy sensible, es que los ataques informáticos no se pueden evitar, pero se puede disminuir el impacto, siempre y cuando se mantenga actualizados los mecanismos preventivos, con esto lograríamos proteger y corregir deficiencias en los sistemas y otros problemas técnicos, que pueden ser vulnerables.

¡Lo que debemos generar!!!

Una cultura de seguridad en todas las personas, ya que en una empresa no solo el Departamento Informático, es responsable del cuidado de la información, lo es cada persona, ya que tienen la responsabilidad, el compromiso y la aceptación, para aplicar los mecanismos preventivos, con esto se lograría que la información institucional y personal este a buen recaudo.

De los diferentes mecanismos (Preventivos, Correctivos, Detectivos y Disuasivos) que existen para la Seguridad Informática, **los preventivos son los más fundamentales** y a la vez para el usuario son vistos como una pérdida de tiempo, incluso se consideran como costos extras, debido a que no tienen una cultura de seguridad en la protección de su información personal, sistemas y demás aplicaciones desde donde se accede. Por lo tanto la prevención, consiste en prever la ocurrencia de un ataque informático, en el monitoreo de la información y sistemas críticos, y la protección de la información que es el activo más importante en una organización.

a) El respaldo de información: La pérdida de información implica un costo y reputación, si no se ha tenido la política de tener respaldos, por tal razón se debe considerar lo siguiente:

- Que formatos de archivos se almacena (Archivos de texto, Base de Datos, Imágenes, Videos y Otros)
- Horario de Respaldo: Seleccionar el tiempo donde no exista mucho tráfico de datos en la red.
- Control de los medios: El tener acceso a respaldos de información es muy importante.
- Tener el respaldo de la información en otro lugar que sea considerado seguro.
- Probar y verificar la funcionalidad de los respaldos, constantemente.

b) Actualización de sistemas: Se debe tener periódicamente actualizado el sistema operativo ya que incluye correcciones de errores, parches de seguridad, etc.

❖Elementos de prevención

c) Antivirus: Debido a la mayoría de ataques por los ciberdelincuentes, se debe tener instalado un antivirus en los equipos tecnológicos para su protección.

d) Firewall: Es un punto muy importante en la seguridad de la información, ya que es un control de seguridad y filtro. Si es para uso personal se debe tener activado el Firewall del S.O y si es para uso empresarial se debe contar con un Firewall Perimetral.

e) Navegación por Internet: Cabe indicar que la mente del ser humano es bien curiosa, por tal razón es necesario saber que se investiga o que se busca, ya que existen sitios web que desean obtener información confidencial del usuario, por eso, es necesario verificar en las barras de direcciones que exista el protocolo https://, esto implica que es un sitio web seguro.

f) Contraseñas: Debe ser robusta, esto implica tener una combinación de símbolos, letras y números, recuerde que no debe usar la misma contraseña para múltiples cuentas.

g) Accesos remotos: Las organizaciones debido a la pandemia (Covid-19) han tenido que hacer cambios obligatorios en su modalidad de trabajar (Tele-Trabajo), por tal razón la seguridad de la información debe poseer Gestión de Roles, Control de Dispositivos, Protección Contra Códigos Malignos, Monitoreo del Trafico de red, Conexiones Seguras, Concientización de los empleados en Seguridad de la Información.

h) Descargas: Tener cuidado con lo que se descarga, porque existen archivos o aplicaciones que son desarrollados por los ciberdelincuentes, con el propósito de dañar y tener el control total del equipo tecnológico y sistema operativo, preferible no abrir ficheros adjuntos sospechosos, ya que si no se ha solicitado se debe eliminar inmediatamente.

i) Correo Electrónico: Desconfiar de los correos con dominios de remitentes desconocidos, ya que podría ser Phishing (Técnica o modalidad que utilizan los ciberdelincuentes para engañar y conseguir que se revele información personal).