BOLETÍN INFORMATIVO DE CIBERSEGURIDAD

"Mecanismos preventivos de Seguridad Informática"

Los mecanismos de seguridad son todas aquellas herramientas que permiten la protección de servicios informáticos y bienes de una empresa pública/privada o usuario. Este tipo de mecanismos pueden ser herramientas físicas, dispositivos o mecanismos no tangibles que permitan resguardas la información; tal como una política de seguridad, protocolos de seguimiento, formas adecuadas de proceder o rutas de acceso delimitadas ante situaciones específicas; es por ello, que estos mecanismos de seguridad también reciben el nombre de controles, ya que dentro de su responsabilidad está el correcto direccionamiento de las acciones a ejecutar y que permitan resguardar la información objeto de protección.

Elementos de prevención:

Antivirus: Debido al incremento de ataques cibernéticos , se debe tener instalado un antivirus en los equipos tecnológicos para la prevención, bloqueo, detección y eliminación de ciertos archivos o ejecutables dañinos que se descargan en el ordenador, sin previo aviso.

Respaldo de información: La pérdida de información implica un costo y reputación, si no se tiene una política de 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.

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 o aplicaciones.

Telf. 2236-092 / Conmutador 3955-900
dntic.direccion@policiaecuador.gob.ec
Dirección Nacional de Tecnologías de la Información y Comunicación
Departamento de Seguridad de las TIC

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.

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, por lo que se recomienda no abrir ficheros adjuntos sospechosos, ya que si no se ha solicitado se debe eliminar inmediatamente.

Correo Electrónico Institucional: 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).

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

Referencias:

a) http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/4928/51257%20-%20Moreno%20Granados%20Diego.pdf?sequence=1&isAllowed=y
b) https://blog.euncet.com/cuales-son-las-normas-de-seguridad-informatica-claves-para-las-empresas/
c) https://www.unir.net/ingenieria/revista/principios-seguridad-informatica/