PROCESOS DE SEGURIDAD INFORMATICA   
ACTIVIDAD I

DICKSON ARLEY GARCIA RINCON

SENA

SERVICIO NACIONAL DE APRENDIZAJE

REDES Y SEGURIDAD INFORMÁTICA

MEDELLÍN

2019

De acuedo a activad planteada se elabora informe sobre empresa con manejo de grandes cantidades de información y las estrategias que se pueden implementar para proteger los activos.

|  |  |
| --- | --- |
| **Nombre de la empresa.** | DDB-Colombia |
| **Productos o servicios que comercializa.** | Marketing Digital |
| **Equipos de informática que manejan por área.** | 20 equipos por área |
| **Necesidades de manejo y almacenamiento de información.** | 200 Teras |
| **Elija el tipo de red que según su criterio debería manejar la empresa descrita.** | LAN, Topología estrella. |
|  | |
| **Estrategia para proteger información** | |
| 1. Encriptación. La encriptación es el proceso que permite convertir datos a una forma o código no reconocible o legible. En nuestra empresa de ejemplo todos los equipos se deben encriptar utilizando la herramienta de BitLocker, mapeada a través del antivirus, el cual envía el mensaje de alerta al usuario para dicha encriptación. Luego se realiza un inventario para comparar que usuarios no hicieron la encriptación y hacerlo manualmente. | |
| 1. Evitar los enlaces sospechosos. Uno de los medios más utilizados paradireccionar a las víctimas a sitios maliciosos son los hipervínculos o enlaces. Evitar hacer clic en éstos previene el acceso a páginas web que posean amenazas capaces de infectar al usuario. Para llevar a cabo esta estrategia se debe consientizar a los usuarios sobre como identificar estos enlaces por medio de charlas o emails informativos. | |
| 1. No acceder a sitios web de dudosa reputación. A través de técnicas de Ingeniería Social, muchos sitios web suelen promocionarse con datos que pueden llamar la atención del usuario – como descuentos en la compra de productos (o incluso ofrecimientos gratuitos). Es recomendable que el usuario esté atento a estos mensajes y evite acceder a páginas web con estas características | |
| 1. Actualizar el sistema operativo y aplicaciones. El usuario debe mantener actualizados con los últimos parches de seguridad no sólo el sistema operativo, sino también el software instalado en el sistema a fin de evitar la propagación de amenazas a través de las vulnerabilidades que posea el sistema. | |
| 1. Descargar aplicaciones desde sitios web oficiales. Muchos sitios simulan ofrecer programas populares que son alterados, modificados o suplantados por versiones que contienen algún tipo de malware y descargan el código malicioso al momento que el usuario lo instala en el sistema. Para evitar este riego, desde la administración central del firewall se puede bloquear estas descargas y así evitar que los usuarios accedan a sitios sospechosos. | |
| 1. Utilizar tecnologías de seguridad. El uso de antivirus antispam y firewall, son importantes para la protección de amenazas. | |
| 1. Evitar la ejecución de archivos sospechosos. A travez de politicas de dominio se puede restringir la ejecución de archivos que no se conozca la seguridad o su procedencia. | |
| 1. Utilizar contraseñas fuertes. Al pensar en mecanismos que contribuyan a la seguridad de los datos, es muy importante utilizar contraseñas robustas, capaces de resistir ataques informáticos. Esta estrategia de seguridad tambien puede administrarse desde el servidor principal. Por medio de políticas en el directorio activo para actualización de contraseña cada 30 dias. | |
| 1. Restricción de acceso a personal no autorizado. Implementación de mecanismos biométricos o magnéticos para evitar el ingreso a personal no autorizado. | |
| 1. Sistema de circuito cerrado. Utilizar cámaras de seguridad en puntos estratégicos como los accesos a la empresa para tener un registro de posibles eventualidades de falla de seguridad. | |