Plan de seguridad - Equipo 2

Clase 25S - Seguridad Informática

Etapa 1

En esta primera se busca fortalecer la seguridad activa, teniendo en cuenta que hay trabajadores que trabajan desde casa; y al manejar información sensible o crítica, se hace necesario asegurar la instalación de antivirus, antiespías y la encriptación de datos.

Esto es aún más necesario, teniendo en cuenta que es posible la conexión a servidores internos o en su defecto a la intranet de la Empresa (como también si la empresa usa un DLP).

Etapa 2

Con la etapa 1 se fortalece la seguridad de la intranet, y para garantizar una cobertura mayor se propone la implementación de buenas prácticas que se harán de manera periódica, tales como:

1. Contraseñas seguras (más de 14 caracteres, incluyendo especiales)
2. Reseteo de contraseñas
3. Escaneo del computador usando el antivirus.
4. Pasos a seguir en los casos donde haya infección (como desconexión de red, reporte al área encargada, entre otros).

Etapa 3

Desde la seguridad física proponemos que la empresa invierta en los siguientes dispositivos o métodos:

1. Sistemas redundantes: teniendo en cuenta que hay empleados fuera de sitio, y que el sistema pudiese fallar, este permitiría que el trabajo en casa se mantenga constante y sin pérdida de la información.
2. Respaldo datos: teniendo en cuenta que la empresa maneja información crítica o sensible, se hace necesario tener un respaldo en los casos donde haya secuestro, hurto o extorsión de la información ya que está puede generar altas pérdidas operacionales.
3. Teniendo en cuenta que los servidores de la Empresa y otros dispositivos críticos de la operación se encuentran en la planta/oficina, se propone la instalación de un UPS para evitar el cese de la operación.
4. Instalación de SSTV en las zonas vulnerables informáticas como servidores o plantas eléctricas.

Etapa 4 = “Mejor prevenir que lamentar”

En esta etapa desplegaremos una serie de simulacros donde los empleados se verán enfrentados en situaciones de vulnerabilidad como puede ser ingreso de malwares que no sólo han afectado al sistema, sino que han robado información personal de los empleados. Los líderes de cada área estarán al tanto y una vez se describa que es un simulacro, estos explicarán cuales son los protocolos a seguir como las buenas prácticas para así evitar que el riesgo se materialice.

De igual forma, se llevarán a cabo auditorías internas para valorar el uso de las buenas prácticas y normativas que la empresa así lo defina.