

GERENCIA DE SEGURIDAD INFORMÁTICA

Estimados,

Ante los recientes hechos de inseguridad que ha sufrido la empresa, se ha contratado una consultoría para la configuración e implementación de una serie de soluciones que han sido aprobadas por la dirección general. a saber:

Se está armando un centro único de autenticación Single Sign-on con 2FA para un mayor control de todos los usuarios de la compañía, la cual tendrá como objetivo la implementación de una política de contraseña segura que consta de tener un tipo de contraseña que se ajuste a los requerimientos modernos que tienen que ver con una longitud y combinación de caracteres especiales entre mayúsculas, minúsculas y números con un segundo factor de autenticación. La misma tendrá un vencimiento y renovación cada 45 días, sin excepción.

Segregación y segmentación de usuarios

Esto vendrá acompañado de un modelado de roles y perfiles en nuestro AD para una correcta segregación de funciones y separación de ambientes.

Firewall:

Asimismo se compró un FireWall perimetral que tendrá, entre otras, la función de concentrador de VPNs para poder ingresar en forma remota a la LAN con un doble factor de autenticación configurado.

Control de acceso biométrico

Para el personal que hace trabajo presencial y para los mixtos, se están instalando tres escáneres de huellas dactilares como barrera física para el ingreso a las oficinas y al DataCenter. Este acceso biométrico ya fue autorizado por el CEO.

Solución de Antivirus

Se instalará por política en todas los activos de la empresa un antivirus corporativo de uso obligatorio.

Cloud Backup

Implementación de un sistema de backup diario, semanal y mensual con guarda por cinco años. todo en un servicio en la nube, administrado por el área de administradores y que saldrá por una regla en el nuevo firewall perimetral.

Data Center

Se está llevando a cabo una reingeniería en el DC para separar las funciones de los servidores, así como Bases de Datos, file server y Web servers, entre otros. Se separarán en tres ambientes. Desarrollo, testeó y producción.

Ancho de banda

Se contrataron tres ISPs con un mayor ancho de banda y conexión redundante para cubrir la demanda de internet durante las videoconferencias.

Redes WiFi

Se aseguró la red Wifi y se forzó su autenticación contra el AD de la compañía. Con lo cual nadie, no autorizado, podrá acceder a la LAN a través del WiFi.

Se implementaran nuevas políticas para la seguridad y la continuidad del negocio:

Política de backup

Política de DRP

Política de Gestión de Incidentes

Política de Ciber Riesgo, Inteligencia de amenazas y comité de crisis.

Política de cifrado de disco, entre otras.

Y realizar una serie de pruebas al personal, con el fin de corroborar el conocimiento y falencias que presentan. La idea es fortalecer aquellos puntos vacíos de conocimiento necesarios para el puesto y capacitarlos.

A su vez, se realizarán campañas de concientización para todo el personal, correspondientes a los ejes de seguridad.

Queda usted debidamente notificado.

ATTe.: La empresa.