1. ¿Cuál es la importancia de establecer políticas de seguridad en una empresa?

Un punto importante es lograr los objetivos organizacionales soportados en el área de IT. Y cumplir con los criterios de preservar los atributos de la información que son: integridad, privacidad, exactitud y disponibilidad.

1. ¿Qué proceso se debe tener en cuenta después que un usuario permite que otras personas tengan acceso al equipo, sin tener en cuenta las políticas de seguridad implantadas en la empresa?

Es necesario que las violaciones a las políticas de seguridad de la información sean clasificadas, con el fin de aplicar medidas correctivas conforme con los niveles de clasificación definidos y mitigar posibles afectaciones contra la seguridad de la información. Las medidas correctivas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, si así lo ameritan.

1. Como administrador de una red tecnológica, ¿qué controles se deben establecer para proteger el software de una empresa?

Algunos controles que se podrían establecer serian, no instalar programas o máquinas virtuales sin la autorización de la Dirección de Tecnología. El software debe estar siempre debidamente soportado por una licencia de uso. La Dirección de Tecnología podría hacer inventarios remotos o presenciales sobre el software instalado en las máquinas de la empresa para verificar que no haya software no autorizado. Considerar las irregularidades como falta grave y ser reportadas a la Dirección de Gestión Humana.

1. Desde el mismo rol, ¿qué controles establece usted para asegurar que los usuarios de la empresa protejan la información?

Para asegurar que los usuarios protejan la información se puede realizar campañas de consientizacion. También restringir el ingreso de computadores personales sin autorización. Restringir cualquier intento de copia de información de la compañía a equipos personales.

1. Una de las políticas de seguridad informática, recomienda efectuar copias de seguridad a la información (backup). Como administrador de una red tecnológica en una empresa, ¿cada cuánto recomendaría efectuar este proceso?, ¿por qué?

Se debe mantener una copia de seguridad actualizada semanalmente de la información de los aplicativos claves de la empresa y en un lugar externo a las instalaciones. Actualmente existen servicios en la nube que brindan alta seguridad de los datos y fiabilidad en el respaldo. También por medio de estas herramientas las copias de seguridad se pueden llevar a cabo luego de realizar cambios en cualquier archivo. Otra función que ofrecen estos servicios es un versionamiento de los cambios y una consola de administración que ayuda a monitorizar todos los usuarios, permisos y políticas para compartir archivos. Si no existe el presupuesto para estos servicios también se puede usar una ruta con Time Machine para Mac o de backup de Windows automática.

1. RTA:

La información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades mas significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad. Dicho esto cabe resaltar que la responsabilidad del administrador de la red informática es de suma importancia.