



## ANÁLISIS DEL ¿PORQUE LA INFORMACIÓN ES EL ACTIVO MÁS IMPORTANTE EN UNA INSTITUCIÓN?

**Descripción:**

**Nivel de Importancia:** ALTA (4)

Tradicionalmente el soporte de la información era solo en papel, posteriormente fueron los soportes magnéticos y hoy en día los soportes electrónicos. La información ha llegado a ser considerada como el ACTIVO más valioso dentro de las empresas e instituciones, en virtud que juega un papel muy importante a la hora de la toma de decisiones y definición de nuevas estrategias de negocios.

En este contexto los avances tecnológicos están transformando la forma de hacer negocios, las empresas e instituciones interaccionan con clientes, con proveedores y con la administración a través de correo electrónico e Internet. Muchas empresas e instituciones también se relacionan a través de redes sociales, comparten documentos en la nube, disponen de página web o venden desde tiendas online. La generación y el intercambio de documentos en formato digital son imprescindibles.

En su día a día las empresas e instituciones manejan información de clientes, de marketing, de recursos humanos, de productos, de facturación, de movimientos financieros, etc. Información crítica que, si se altera, destruye, divulga o por alguna causa resulta inaccesible puede causar graves pérdidas a las empresas e instituciones.

La información ya sea almacenada en el equipo, en dispositivos externos, en servidores (de correo, de almacenamiento, etc.) o en servicios en la nube son ACTIVOS para las empresas e instituciones, es decir, tiene mucho valor y deben protegerse.

El establecimiento de procedimientos, planes y políticas de almacenamiento, conservación, recuperación y borrado es esencial para garantizar la seguridad de la Información que constituye uno de los Activos más importantes para las empresas e instituciones.

### Recomendaciones para la seguridad de la información:

Las empresas, instituciones y las personas debemos implementar acciones para proteger y evitar comprometer la seguridad de la información:



- Utilizar contraseñas fuertes que contengan mayúsculas, minúsculas y números. Tienen que ser fáciles de recordar para el propietario y difíciles de adivinar por otros.
- No compartir ni usar la misma clave para las distintas aplicaciones, cuentas, plataformas, etc.
- Leer con cuidado los emails que recibimos y verificar que los sitios remitentes sean legítimos.
- Cuando por teléfono ofrezcan premios, préstamos o beneficios importantes, nunca se deben proporcionar datos de tus cuentas y/o tarjetas operaciones.



- Las instituciones financieras nunca llamarán para pedirte contraseñas ni datos de tu cuenta.
- No uses equipos públicos o de terceros para acceder a las aplicaciones o sitios financieros.
- Para realizar alguna compra o transacción financiera online, siempre se debe verificar que la dirección web comience por «https://». Este código certifica que se trata de una página que cumple con las normas de seguridad establecidas.
- Usar un antivirus en cada uno de los dispositivos y, sobre todo, realizar un análisis completo por lo menos una vez por semana para detectar cualquier tipo de anomalía.
- La información valiosa, debe estar cifrada mientras no se usa directamente. Es decir: “si está almacenado, cífralo”.
- Realizar copias periódicas de seguridad, las copias de los datos y los sistemas constituyen la última línea de defensa (y la mejor) ante los ciberdelincuentes.
- Verificación de las cuentas de usuario al menos una vez al año para eliminar permisos que ya no sean apropiados.

