20211210, Nota Informativa, ciberseguridad sobre correo electrónico.

En virtud de mis compromisos contractuales, seguidamente os traslado una serie de principios y recomendaciones sobre el correo electrónico.

El **CCN-CERT (Centro Criptológico Nacional)** en el documento titulado "principios y recomendaciones sobre ciberseguridad", al que ya nos acercamos en las dos últimas Notas Informativas, dedica un apartado al correo electrónico que considero puede ser de mucho interés. A ello pues.

Actualmente el correo electrónico sigue siendo una de las herramientas más utilizadas por cualquier entorno corporativo para el intercambio de información a pesar de que en los últimos años han surgido multitud de tecnologías y herramientas colaborativas para facilitar la comunicación y el intercambio de ficheros.

El incremento y efectividad de la ingeniería social para engañar a los usuarios por medio de correos electrónicos ha modificado el paradigma de la seguridad corporativa.

Actualmente los cortafuegos perimetrales y la securización de los servicios expuestos a Internet no son contramedidas suficientes para proteger una organización de ataques externos.

Algunas recomendaciones para utilizar el correo electrónico de forma segura:

- No abrir ningún enlace ni descargar ningún fichero adjunto procedente de un correo electrónico que presente cualquier indicio o patrón fuera de lo habitual.

- No confiar únicamente en el nombre del remitente. El usuario deberá comprobar que el propio dominio del correo recibido es de

confianza. Si un correo procedente de un contacto conocido solicita información inusual contacte con el mismo por teléfono u otra vía de comunicación para corroborar la legitimidad del mismo.

- Antes de abrir cualquier fichero descargado desde el correo, hay que asegurarse de la extensión y no fiarse del icono asociado al mismo.

- No habilitar las macros de los documentos ofimáticos incluso si el propio fichero así lo solicita.

- No hacer clic en ningún enlace que solicite datos personales o bancarios.

- Tener siempre actualizado el sistema operativo, las aplicaciones ofimáticas y el navegador (incluyendo los plugins/extensiones instaladas).

- Utilizar herramientas de seguridad para mitigar exploits de manera complementaria al software antivirus.

- Evitar hacer clic directamente en cualquier enlace desde el propio cliente de correo. Si el enlace es desconocido, es recomendable buscar información del mismo en motores de búsqueda como Google o Bing.

- Utilizar contraseñas robustas para el acceso al correo electrónico. Las contraseñas deberán ser periódicamente renovadas y si es posible utilizar doble autenticación.

- Cifrar los mensajes de correo que contengan información sensible.

En todo caso, y como siempre, quedo a vuestra disposición para aclarar cualquier duda sobre la cuestión comentada.

Hecho conforme a mi leal saber y entender, en Manilva a 10 de diciembre de 2021,

ZOTANO SANCHEZ SALVADOR - 32028277H

Firmado digitalmente por ZOTANO SANCHEZ SALVADOR - 32028277H
Fecha: 2021.12.10 08:40:33 +01'00'

Salvador Zotano Sánchez

(Delegado de Protección de Datos Certificado 19-ADK0101 conforme al Esquema AEPD-DPD)