El presente folleto tiene como objetivo sensibilizar y concientizar en la gestión de Seguridad de información de la FEPCMAC

SEGURIDAD DE INFORMACIÓN

¿Qué es la información?

Es el conjunto de datos que es importante para una persona u organización

¿Qué es Seguridad de la información?

Es toda medida preventiva o correctiva que permita resguardar y proteger la información de la organización.

¿Qué tipos de riesgos estamos expuestos?

Phishing

Modalidad de estafa con el objetivo de obtener de un usuario sus datos, claves, cuentas bancarias, números de tarjeta de crédito, identidades, etc. Para ser usados de forma fraudulenta

Ingeniería Social

Es la práctica de obtener de las personas de dentro de las organizaciones información confidencial (números de cuentas o contraseñas)

Correos Cadena

- Pueden ser mensajes enviados por desconocidos, por amigos o parientes bien intencionados.
- Sugiere que habrá consecuencias trágicas si no ejecuta alguna acción.
- Pueden esconder un virus u otra actividad malévola.
- Consumen ancho de banda y espacio de almacenamiento de la cuenta del destinatario.

Sensibilización de la Gestión de Seguridad de Información

FEPCMAC
FEDERACION PERUANA DE CAJAS MUNICIPALES DE AHORRO Y CREDITO

Políticas de Seguridad de información

Es un conjunto de directrices y lineamientos que nos ayudan a garantizar la seguridad de la información en la organización**.**

Todo dato e Información que se maneje en la FEPCMAC, es de propiedad exclusiva deberá protegerse ante cualquier riesgo.

El ingreso y salida de **equipos portátiles** del personal interno y externo deberá ser debidamente autorizado y cumplir los controles de seguridad de vigilancia.

Toda persona que acceda a información electrónica, deberá tener un identificador de usuario, el cual es único, personal, intransferible y de uso obligatorio.

Sólo deberá utilizar el **correo electrónico** para sus funciones asignadas, es importante recordar que todo mensaje de origen sospechoso **deberá ser eliminado** sin abrir el contenido. Está **prohibido:** correos masivos, correos cadenas y uso del correo institucional para fines personales.

Se deberá realizar **copias de seguridad (backup)** de la información que permita mantener la continuidad de las operaciones.

Responsabilidades del Usuario

1. **Bloquear** el acceso a las computadoras ante cualquier ausencia del escritorio.
2. **Elegir adecuadamente** sus contraseñas de acceso a recursos informáticos.
3. **No compartir** los identificadores de usuarios (usuario de acceso a la red o de acceso a las aplicaciones), ni tampoco las contraseñas.
4. **Comunicar** cualquier **incidente de SI** al asistente de soporte de TI a través del correo electrónico o a través del Teléfono (01) 222-4002 Anexo 302.
5. **No dejar** las puertas abiertas de las áreas restringidas, bajo ninguna circunstancia.
6. **No dejar** papeles impresos en las bandejas de salida de las impresoras o en lugares próximos a ellas.
7. **Mantener sus escritorios limpios,** guardar sus documentos y objetos de valor de forma segura.

La seguridad no es responsabilidad solamente de una persona, sino de **toda la organización.**