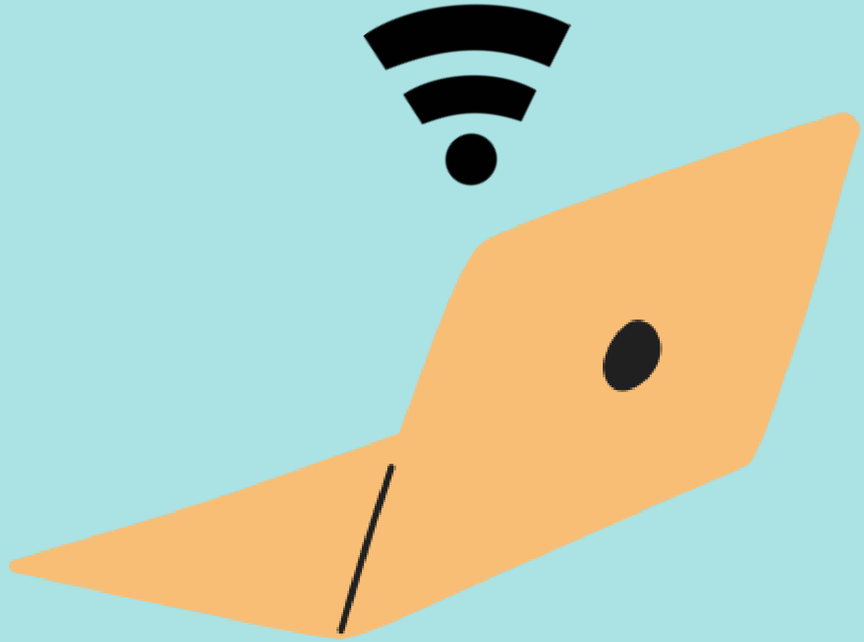
BUENAS PRÁCTICAS EN LA OFICINA

Uso de Recursos y Equipos Informáticos



IMPORTANCIA DE LA SEGURIDAD INFORMÁTICA

Protege la integridad, confidencialidad y disponibilidad de la información.

Garantiza la continuidad del negocio y la confianza del cliente.

SEGURIDAD DE CONTRASEÑAS

Usar contraseñas robustas y únicas.

¿Podemos compartir la contraseña?

¿Solo basta la contraseña?

PREVENCIÓN DE MALWARE Y ATAQUES DE VIRUS

Verificar el funcionamiento del antivirus y estar alerta a los mensajes

Evitar abrir adjuntos sospechosos o que generen duda

No hacer clic en ningún enlace que llegue por medio de un correo

Cuidado con el Phishing

¿Como detectar si un correo es verdadero o no?

Aun así hay riesgo, por eso. Ante la duda, pregunte a sistemas.

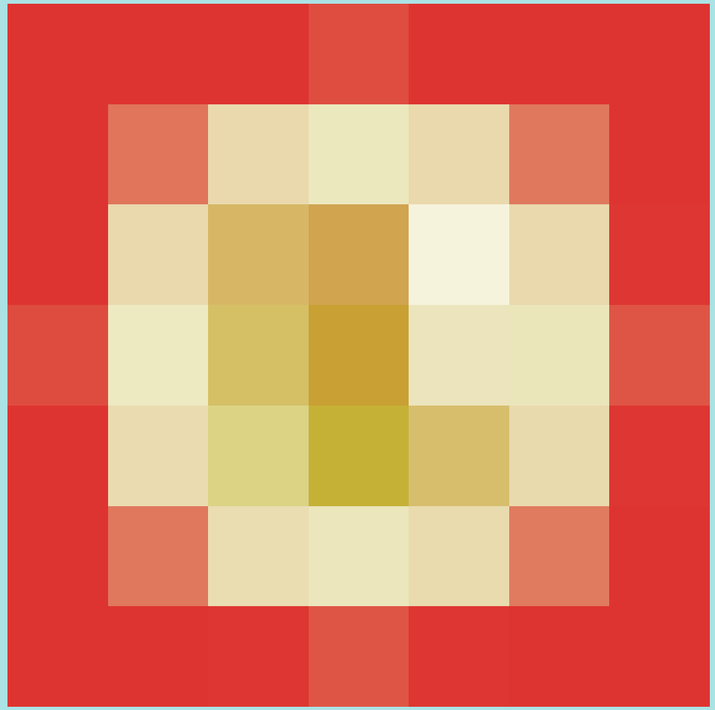
ACTUALIZACIONES DE SOFTWARE Y SISTEMAS OPERATIVOS

Es importante hacer caso a los mensajes que sugieren actualización de nuestros sistemas,
Si le aparece un mensaje que pida actualizar algún programa. Avise a sistemas.

SEGURIDAD FÍSICA DE LOS DISPOSITIVOS

Proteger los dispositivos con contraseñas o biometría.

Evita el acceso no autorizado a través de medidas físicas como cerraduras.



USO SEGURO DEL CORREO ELECTRÓNICO Y NAVEGACIÓN WEB

No abras correos electrónicos o enlaces de fuentes desconocidas.

Utiliza filtros de correo no deseado y software de seguridad web (antivirus)

PROTECCIÓN DE DATOS Y PRIVACIDAD

Usa las carpetas compartidas de manera ordenada.

Limita el acceso a la información según roles y necesidades

COPIA DE SEGURIDAD DE DATOS

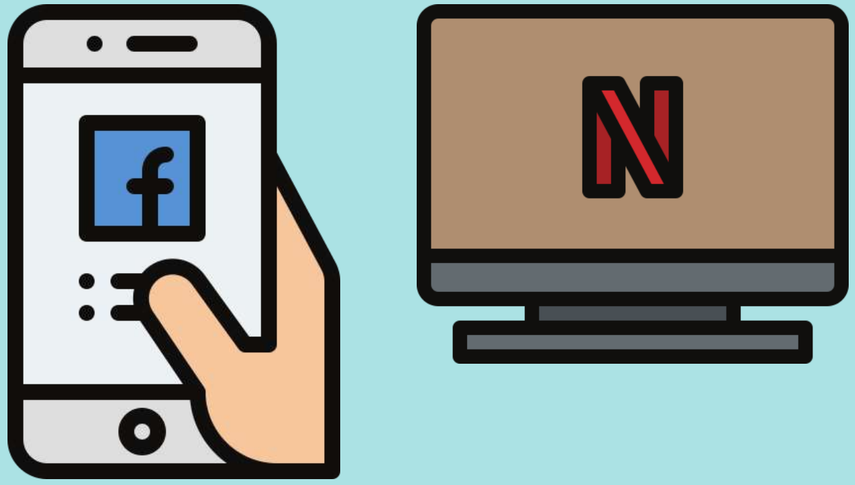
Asegurarnos que nuestra información se encuentre en “mis documentos” y de manera ordenada

Probar eventualmente la restauración de datos.

NORMAS DE USO DE DISPOSITIVOS PERSONALES EN EL TRABAJO

Los dispositivos que les asignamos (PCs, laptops, celulares, thinclients, etc), para las labores de la empresa

No se trata de una exageración. Los recursos de la red, internet, energía, lo usan cerca de 50 dispositivos a la vez en la empresa. El que se use para funciones



EDUCACIÓN SOBRE INGENIERÍA SOCIAL

Tácticas de manipulación utilizadas por los atacantes.

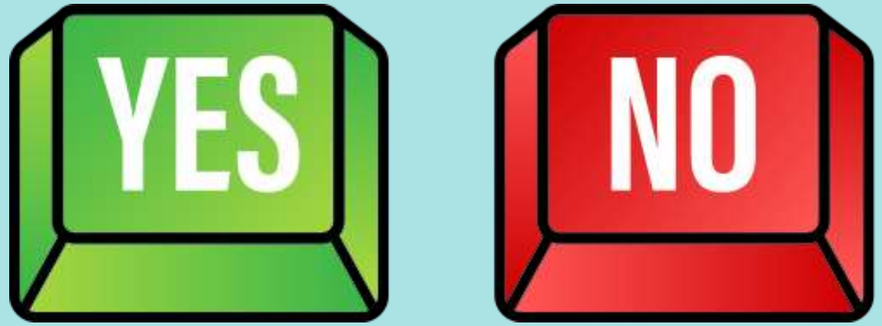
Prudencia al compartir información personal o empresarial.

PROTOCOLOS DE SEGURIDAD FÍSICA Y DIGITAL DE LA OFICINA

Controla el acceso físico a las instalaciones con restricciones

USO ADECUADO DE LOS EQUIPOS Y RECURSOS INFORMÁTICOS

uso responsable de los recursos informáticos.



consecuencias del uso indebido, como la pérdida de productividad y la exposición a riesgos de seguridad.

CONTROL DE LICENCIAS DE ACCESO

Ychiscom

Labeltraxx