

# 5 HABITOS PARA MANTENER LA LINEA DE DEFENSA



## Piensa antes de hacer click

El phishing sigue siendo la principal estrategia de los ciberatacantes. Envían millones de emails maliciosos.



Lee cuidadosamente los emails, pasa el mouse por encima de los URL y sospecha de todas las solicitudes de datos delicados.

## Presta atención al entorno

Y mantente alerta, Si trabajas en H.O. Asegúrate de que tus dispositivos no se dañen, se pierdan o se los roben.



Si trabajas en una zona pública o en el transporte, prioriza la privacidad y asegúrate de que nadie pueda ver tu pantalla.



## Respetar el acceso

Desde las credenciales de inicio de sesión (usuario y contraseña) hasta las tarjetas de acceso que te permiten entrar a zonas seguras o restringidas.



Asegúrate de bloquear las estaciones de trabajo si no las usas, siempre utiliza contraseñas seguras y únicas para cada cuenta.

## Informa los Incidentes

Ya sea una puerta de seguridad abierta, un individuo desconocido merodeando en la oficina, un email sospechoso, una computadora o teléfono que no funcionen bien.



Los incidentes se producen, informarlos ayuda a mitigar los daños y a reducir el nivel de riesgo. Si ves u oyes algo, ¡infórmalo!



## Cumple las políticas de seguridad

Las políticas establecen estándares sobre cómo se recopilan, almacenan, transfieren y destruyen los datos cuando ya no se necesitan. Existen para garantizar la privacidad de los empleados, clientes, consumidores y socios.



El incumplimiento de las políticas podría dar lugar a violaciones de seguridad de datos y otros incidentes contra la seguridad.

No todos los hackers poseen la capacitación técnica necesaria para lanzar ciberataques avanzados. Muchos se enfocan en crear estrategias para impactar a los usuarios y hacer que caigan en la trampa. Por eso, a los usuarios como tú se les llama la "última línea de defensa".

TU LOGO AQUÍ

