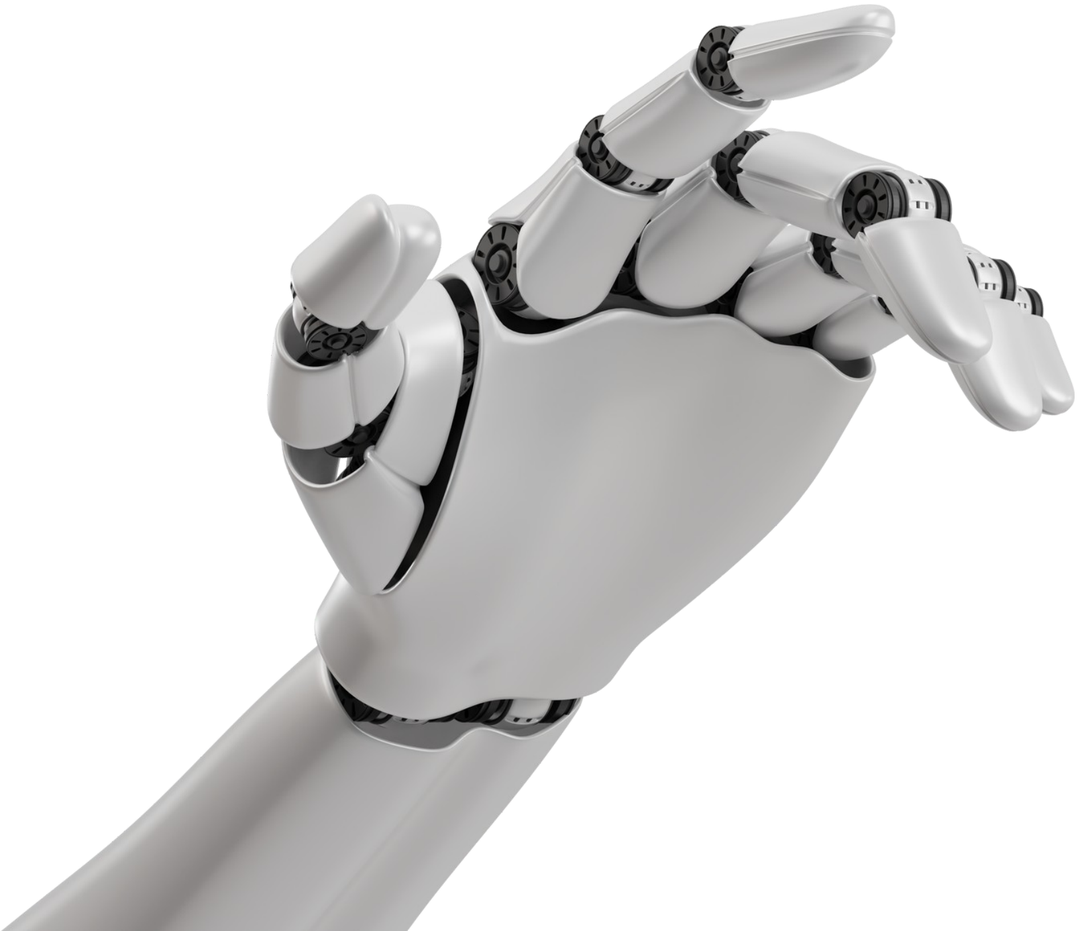
UVM Lomas Verdes



ERROR HUMANO

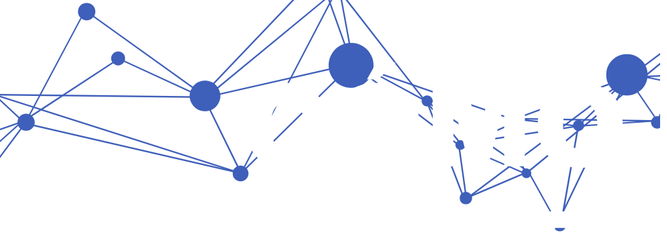
Sorprendentemente, un gran porcentaje de las brechas de datos se debe a errores humanos, como configuraciones incorrectas de seguridad, credenciales débiles o caer en trampas de phishing.

VULNERABILIDADES DE SOFTWARE

Las fallas de seguridad en el software son explotadas continuamente. Mantener los sistemas y aplicaciones actualizados con los últimos parches de seguridad es crucial.

PHISHING Y RANSOMWARE

Siguen siendo los métodos más efectivos para obtener acceso inicial. El phishing de spear (dirigido) y el ransomware como servicio (RaaS) están en aumento, facilitando los ataques incluso a actores menos sofisticados.



Contactar a las Autoridades

Reportar el incidente a las fuerzas de seguridad o entidades regulatorias locales (en algunos países existen líneas telefónicas para reportar fraudes).

Notificar a las Entidades Financieras

Si los datos robados son bancarios, se debe notificar inmediatamente al banco o proveedor de servicios financieros para bloquear o cambiar las cuentas.

Monitoreo de Crédito

Considerar la contratación de servicios de monitoreo de crédito para detectar cualquier uso indebido de la información personal.

Ante el aumento de los robos de información, gobiernos de todo el mundo están implementando leyes de protección de datos más rigurosas (como el GDPR en Europa o la LFPDPPP en México), con multas millonarias para las empresas que no cumplan.

Las organizaciones no solo se están centrando en prevenir ataques, sino también en desarrollar la capacidad de recuperarse rápidamente después de una brecha, minimizando el daño.

Para las empresas, la ciberseguridad ha pasado de ser una preocupación técnica a una prioridad de negocio estratégica, reconocida por las juntas directivas.