CÁPSULA DE SEGURIDAD

PROTECCIÓN DE LA INFORMACIÓN Y EL ENTORNO

Protocolo de Defensa Integral para
el Equipo de Buenas Prácticas

DOCUMENTO DE LECTURA OBLIGATORIA PARA PROFESIONALES DEL RIESGO

NUESTRA SEGURIDAD YA NO TERMINA EN EL PUESTO DE CONTROL

Saludos, equipo. Como profesionales del riesgo, sabemos defender el perímetro físico. Sin embargo, hoy la amenaza ha mutado: **el riesgo también es digital.**

Un error en la gestión de la información es tan peligroso como una brecha en la cerca perimetral. La seguridad física y la digital hoy son una sola misión.

ALERTA DE AMENAZA ACTIVA: LA TRAMPA DEL PHISHING

MODUS OPERANDI

- Se han detectado campañas de mensajes falsos circulando actualmente.
- El vector de ataque principal son notificaciones fraudulentas sobre “Jurados de Votación” y otros trámites administrativos.
- Objetivo: Engañar al personal para robar credenciales o instalar software malicioso.

ANATOMÍA DEL ATAQUE: INGENIERÍA SOCIAL

ENTRADA DIGITAL
Clic en enlace falso

ROBO DE INFORMACIÓN
Obtención de datos tácticos

VULNERABILIDAD FÍSICA
Criminales conocen el esquema

El objetivo del atacante no es siempre el dinero inmediato. La Ingeniería Social utiliza los datos que entregamos inocentemente para identificar vulnerabilidades en nuestros esquemas de seguridad física.

Tu información personal es la llave maestra de la operación.

ASIGNACIÓN DE RESPONSABILIDADES POR ROL

Protocolos de defensa específicos para cada unidad operativa. Ubique su cargo.

VIGILANTES Y ESCOLTAS

OPERADORES DE MEDIOS

SUPERVISORES Y COORDINADORES

DIRECTORES Y JEFES

PROTOCOLO: VIGILANTES Y ESCOLTAS

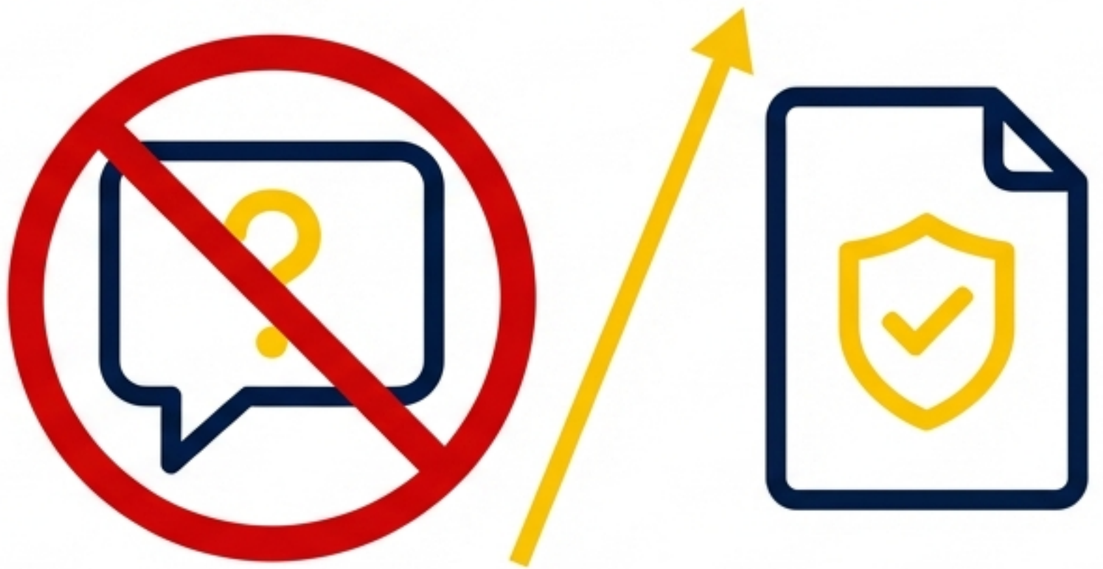
- **INSTRUCCIÓN:** Eviten publicar fotos en tiempo real usando el uniforme.
- **RIESGO:** No muestren la ubicación exacta de sus servicios en redes sociales personales.
- **RAZONAMIENTO:** Al revelar su ubicación y equipamiento, le están entregando al enemigo un mapa de nuestras vulnerabilidades. Mantengan su posición confidencial.

PROTOCOLO: OPERADORES DE MEDIOS TECNOLÓGICOS

- **INSTRUCCIÓN:** Mantengan la alerta máxima sobre correos o enlaces sospechosos que lleguen a los equipos de monitoreo.
- **CONSECUENCIA:** Un solo clic erróneo no es solo un virus en un computador; puede comprometer toda la red de cámaras y sistemas de alarmas.
- **ACCIÓN:** Si duda del origen de un mensaje, no interactúe. Reporte inmediatamente.

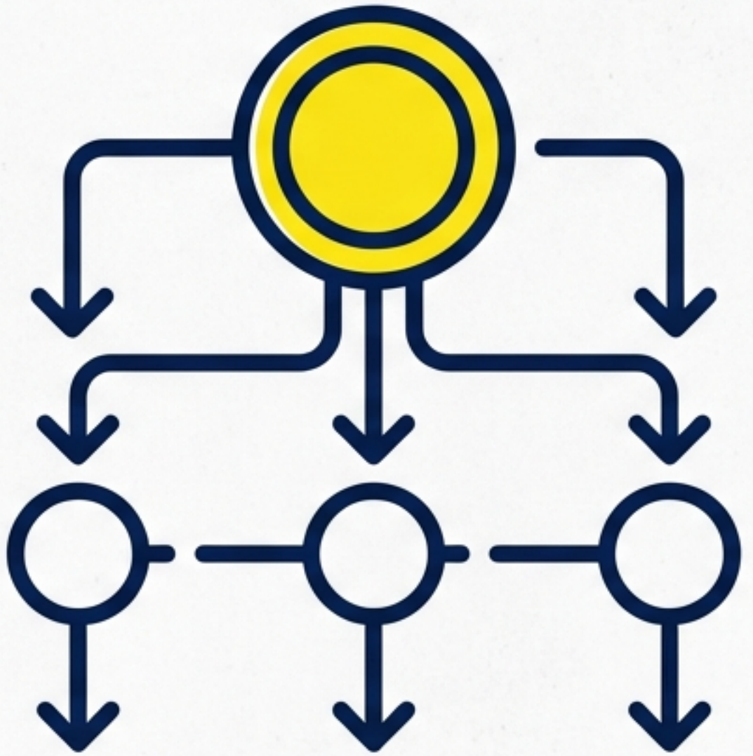
PROTOCOLO: SUPERVISORES Y COORDINADORES

- **INSTRUCCIÓN:** Verifiquen siempre la fuente de la información antes de difundirla en los grupos de mando.
- **FILTRO:** Detengan la cadena de desinformación.
- **CANALES OFICIALES:** Usen exclusivamente canales y páginas oficiales. Busquen la extensión **.gov.co** para trámites gubernamentales.



PROTOCOLO: DIRECTORES Y JEFES DE SEGURIDAD

- **INSTRUCCIÓN:** Fomenten activamente la cultura de la ciberseguridad en sus equipos.
- **VISIÓN ESTRATÉGICA:** Entiendan y transmitan que la seguridad física y la digital hoy son una sola disciplina.
- **MANDATO:** El liderazgo es la primera línea de defensa.



EL ESLABÓN DE CIERRE

EN SEGURIDAD, EL ESLABÓN MÁS DÉBIL SUELE SER EL EXCESO DE CONFIANZA.

La tecnología puede fallar, pero el criterio del operador debe mantenerse intacto.

MISIÓN CUMPLIDA: INTEGRIDAD TOTAL

¡Protejamos nuestra información para proteger nuestra operación!

#SeguridadIntegral #Ciberseguridad #BuenasPracticas #SeguridadPrivadaColombia