Tus Credenciales, Nuestra Fortaleza.

El Rol Clave de Cada Colaborador en la Seguridad de Grupo Palmas

Grupo Palmas

Departamento de TI

La Seguridad Digital No es un Departamento. Es una Cultura.

La seguridad es una responsabilidad compartida. Cada empleado es la primera línea de defensa. Una cultura de seguridad fuerte, basada en el conocimiento y la vigilancia, es el pilar para proteger la integridad de nuestros sistemas.

El 81% de las brechas de seguridad corporativas se deben a contraseñas comprometidas (Fuente: Verizon Data Breach Report, 2025).

Un acceso no autorizado puede desencadenar pérdidas millonarias y un daño irreparable a la reputación de la empresa.

Tú eres nuestra primera línea de defensa.

El Riesgo es Real: Cuando una Sola Credencial Comprometió a un País.

Estudio de Caso: RENIEC (2025)

¿Qué ocurrió?

- Una cuenta autorizada del Ministerio del Interior **accedió indebidamente** a la base de datos de RENIEC.
- Se extrajeron **datos sensibles**: DNI, nombres completos, direcciones, firmas e incluso fotos.
- El incidente se filtró, y las bases de datos terminaron circulando en foros y plataformas no oficiales.

Lecciones Críticas de una Brecha Anunciada.

El Punto Débil

- Uso indebido de credenciales válidas.
- No se aplicaron controles fuertes de autenticación (MFA).
- Falta de monitoreo y alertas ante uso anómalo.
- Exceso de privilegios para una sola credencial.

Nuestro Plan de Acción

- Toda contraseña debe ser robusta y protegida, incluso si es “interna”.
- Toda credencial con acceso a datos sensibles debe tener Doble Autenticación (MFA) como mínimo.
- Una falla en el manejo de accesos puede comprometer a toda la organización.

Nuestro Protocolo: El Escudo de Acceso Corporativo.

Nuestro protocolo de acceso está diseñado para maximizar la seguridad. Entender cada paso garantiza la protección de la información.

Usuario Único

Ingreso del usuario único asignado a cada colaborador.

Clave Robusta

Introducción de una clave fuerte y secreta, cumpliendo con los estándares.

Verificación MFA

Para accesos críticos, se requiere verificación de múltiple factor (MFA).

Acceso o Bloqueo

Acceso autorizado o bloqueo tras intentos fallidos, salvaguardando la integridad.

Forjando una Contraseña Inquebrantable.

La fortaleza de una clave es su primera línea de defensa.

Pilar 1: Longitud y Complejidad

Mínimo 12 caracteres con una combinación de mayúsculas, minúsculas, números y símbolos.

Pilar 2: Cero Datos Personales

Mínimo 12 caracteres con una combinación de mayúsculas, minúsculas, números, números y símbolos.

No utilizar fechas de nacimiento, nombres, ni palabras comunes o secuencias fácilmente adivinables (ej: 123456, qwerty).

Pilar 3: Actualización Constante Cambiar la clave cada 90 días, o inmediatamente si se sospecha de su compromiso.

Hábitos de un Guardián Digital (Parte I)

Principio 1: Confidencialidad Absoluta

Nunca compartir usuario ni clave con nadie, ni con compañeros ni superiores. Las credenciales son estrictamente personales e intransferibles.

Principio 2: Almacenamiento Inteligente

Evitar escribir claves en notas físicas o en archivos digitales sin protección. Utilice solo los métodos seguros de almacenamiento que provee la compañía.

Hábitos de un Guardián Digital (Parte II).

Principio 3: Usa las Herramientas Autorizadas.

Hacer uso de los gestores de contraseñas corporativos autorizados, que ofrecen un entorno seguro para guardar y gestionar sus claves.

Principio 4: Cierra Siempre la Puerta.

Cerrar siempre la sesión al finalizar el uso de cualquier sistema, especialmente en dispositivos compartidos o públicos.

Identificando las Amenazas: Tu Radar de Riesgos

Amenaza 1: Phishing

Intentos de fraude para obtener información confidencial.

Prevención

No ingresar usuario y clave en enlaces sospechosos. Siempre verificar la autenticidad de los correos y las URLs antes de hacer clic.

Amenaza 2: Reutilización de Claves

Usar la misma clave en múltiples plataformas. Si una se compromete, todas están en riesgo.

Prevención

Utilizar una clave única y robusta para cada sistema y aplicación corporativa.

Amenaza 3: Sesiones Abiertas

Dejar sesiones activas en dispositivos compartidos, permitiendo el acceso a terceros.

Prevención

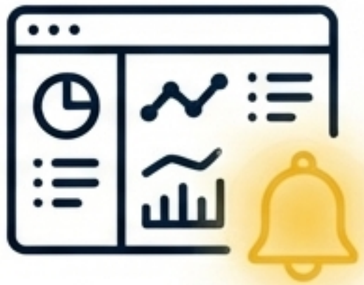
Cerrar siempre la sesión al alejarse del equipo o al finalizar la jornada.

Nuestra Armadura Corporativa: Las Herramientas que Te Protegen.

La empresa pone a su disposición diversas herramientas para fortalecer la seguridad de su acceso y proteger la información corporativa.

Autenticación Multifactor (MFA)

Añade una capa extra de seguridad. Requiere dos o más métodos de verificación para acceder.



Monitoreo en Tiempo Real

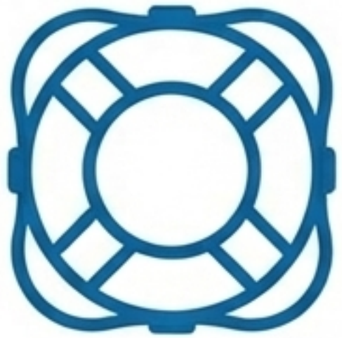
Sistemas que detectan y alertan sobre actividades inusuales o sospechosas en sus accesos.

Capacitación Continua

Programas de formación para mantener a los empleados actualizados sobre las últimas amenazas y mejores prácticas.

¿Clave Olvidada? Proceso de Rescate Seguro.

Nuestro proceso de recuperación está diseñado para ser seguro y eficiente, garantizando que solo usted pueda restablecer su acceso.



Opción 1: Portal Mesa de Ayuda

Iniciar el proceso de recuperación de forma autónoma a través del portal corporativo.

Opción 2: Canal Telefónico

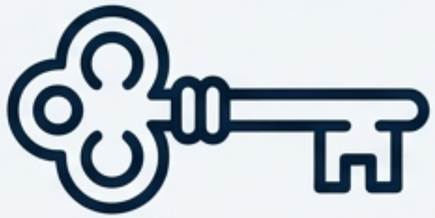
Puedes llamar al número de mesa de ayuda: 01-645-2080.

Opción 3: Soporte TI en Sede

Puedes solicitar el soporte del personal de TI asignado a tu sede.

Tu Playbook de Seguridad: 4 Reglas de Oro.

1.



CREA CLAVES ÚNICAS Y ROBUSTAS.

Usa el método de los 3 pilares: longitud, complejidad y sin datos personales.

2.

ACTIVA Y USA SIEMPRE EL MFA.

Es tu capa de seguridad más importante contra el acceso no autorizado.

3.

DESCONFÍA Y VERIFICA.

Ante cualquier solicitud sospechosa, detente y verifica su autenticidad.

4.

REPORTA ANOMALÍAS DE INMEDIATO.

Tu vigilancia es clave para detectar amenazas a tiempo.

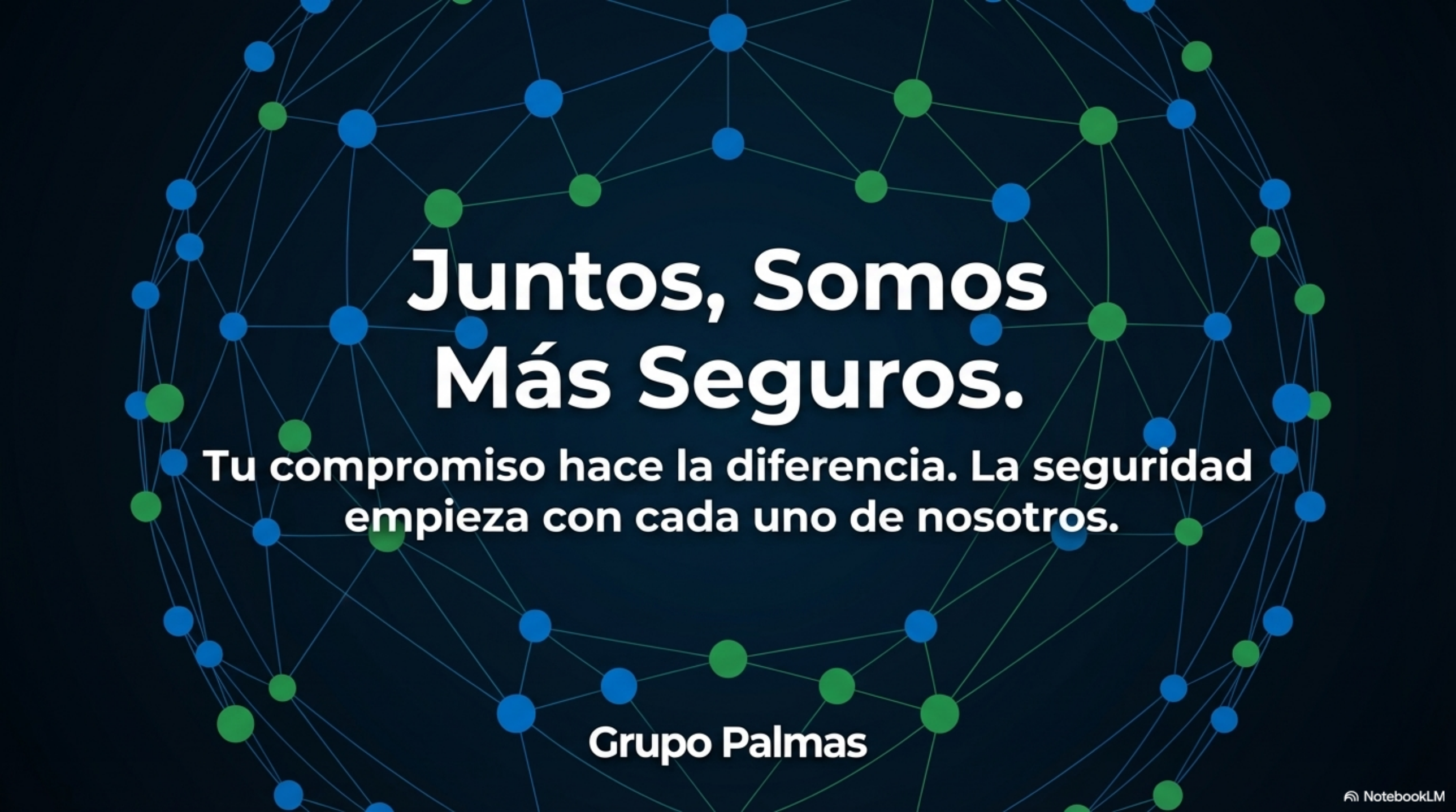
Tu Compromiso: El Activo Más Valioso.

La seguridad de nuestra empresa es un esfuerzo colectivo. Cada acción que tomas con tus credenciales tiene un impacto significativo.

Tu Llave a la Seguridad: Protege tu usuario y clave como el activo más valioso que son.

Adopta las Buenas Prácticas: Aplica siempre las mejores prácticas que hemos revisado para proteger tus credenciales.

Participa y Reporta: Participa activamente en las capacitaciones y reporta cualquier anomalía o sospecha de inmediato.


Juntos, Somos Más Seguros.
Tu compromiso hace la diferencia. La seguridad empieza con cada uno de nosotros.
Grupo Palmas
NotebookLM

Gracias.

¿Necesitas Ayuda?

Mesa de Ayuda TI

Teléfono: 01-645-2080

Portal: [URL for the corporate help desk portal]

Departamento de TI