¡Bienvenidos!

Taller Buenas prácticas de seguridad en tu plataforma BUK 🔐

buk Gestión de Personas

Equipo Buk

David Diaz
Customer Solutions Education

Felipe Cifuentes
Information security engineer

William Barrios M
Customer Solutions Education

¿Qué es la seguridad?

y porque nos importa tanto

buk Gestión de Personas

¿Qué es seguridad de la información?

La seguridad, en términos generales, se refiere a la **protección** contra cualquier **riesgo**, amenaza o peligro que pueda afectar la **disponibilidad, integridad o confidencialidad** de la información que requiere la organización para operar. Puede abarcar diversos aspectos, desde la **seguridad física** hasta la seguridad en el ámbito **digital**.

¿Es lo mismo que la Ciberseguridad?

¡Son muy parecidos! La Ciberseguridad se enfoca únicamente en los sistemas, redes y datos que se encuentran en espacios cibernéticos

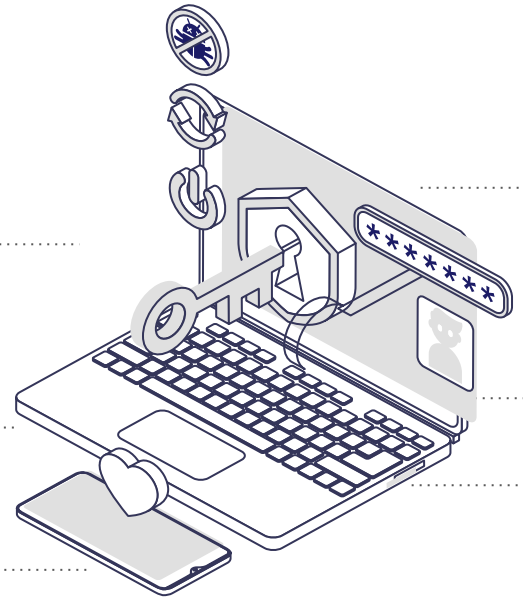
buk

Amenazas comunes: ¿Qué nos acecha?

INGENIERÍA SOCIAL
Manipulación psicológica para engañar a las personas y obtener información confidencial o hacerlas realizar acciones inseguras.

PHISHING
Técnica de engaño donde se hacen pasar por entidades confiables para robar información personal.

ATAQUE AL CEO
Fraude en el que los atacantes se hacen pasar por altos ejecutivos, generalmente el CEO, para engañar a empleados y obtener transferencias de dinero o información confidencial.



MALWARE
Software malicioso diseñado para dañar, explotar o comprometer dispositivos y redes.

RANSOMWARE
Es un software que cifra archivos y exige dinero a cambio de desbloquearlos.

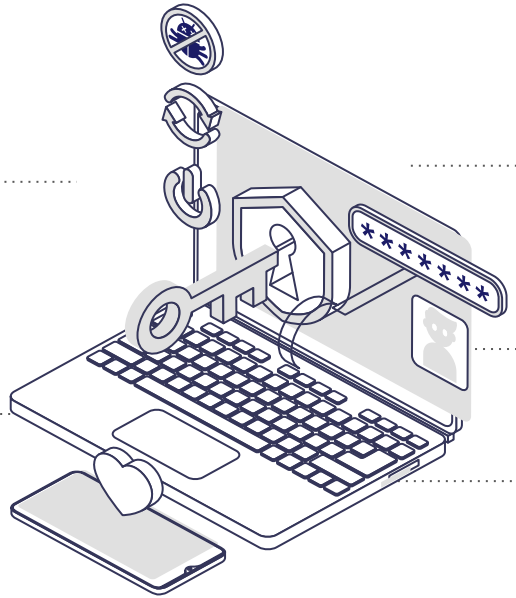
SPYWARE
Son programas que espían las actividades en línea de los usuarios, para robar contraseñas o registrar lo que escriben.

Vulnerabilidades: Nuestras puertas abiertas

“Los incidentes de seguridad no siempre empiezan con un hacker encapuchado. A veces... somos nosotros.”

Política de contraseña Débil
El uso de contraseñas débiles o compartidas es una vulnerabilidad importante. Esto incluye contraseñas como “Buk2025” o genéricas

Usuarios Genéricos
El uso de una misma cuenta por varias personas dificulta el seguimiento y la responsabilidad



Usuarios Genéricos y Privilegios excesivos
El uso de cuentas compartidas o la asignación de más permisos de los necesarios

Acceso sin autenticación en múlti- capas
Depender únicamente de una contraseña para acceder a la plataforma. Si una contraseña es robada, la cuenta queda expuesta.

Ausencia de un Sistema de Trazabilidad
No tener un registro de cambios dentro de la plataforma podría dificultar la detección de responsabilidades en caso de un incidente de seguridad.

Situaciones de riesgo

Error humano

- Un administrador asigna por error un privilegio excesivo a un colaborador, dándole acceso a información confidencial que no debería ver.
- Un colaborador elimina accidentalmente datos críticos de la plataforma.

Mala gestión de contraseñas

- Colaboradores utilizan contraseñas débiles o fáciles de adivinar ("MiEmpresa2024").
- Cuenta comprometida por un phishing, ya que no tiene una segunda capa de seguridad

Exposición involuntaria de información

- Se utilizan cuentas genéricas o se permite que las cuentas se compartan
- Se le otorgan permisos de forma masiva a todos los usuarios, sin considerar el principio de mínimos privilegios

Recomendaciones: buenas prácticas

Eviten **usuarios genéricos** y usen cuentas personales únicas

Apliquen el principio de **mínimos privilegios**

Utiliza **doble factor** de autenticación siempre que esté disponible

Mantén todos tus software y equipos con las **actualizaciones al día**.

Utilizar el **Historial de cambios** para tener visibilidad de las acciones que se realizan

Utiliza un método de **respaldo** adecuado a la criticidad de tu información y sistemas

buk

¿Conoces Single Sign-On?

buk Gestión de Personas

Single Sign - On.

Es un protocolo de autenticación que permite a los usuarios acceder a múltiples aplicaciones y servicios utilizando las mismas credenciales de inicio de sesión. En lugar de tener que recordar diferentes nombres de usuario y contraseñas para cada aplicación, SSO permite a los usuarios autenticarse una sola vez y luego acceder a todas las aplicaciones y servicios sin necesidad de volver a ingresar sus credenciales.

Principales beneficios de habilitar SSO en Buk.

- ✅ Seguridad reforzada desde el primer acceso
- ✅ Mejor experiencia para los usuarios
- ✅ Control total de accesos y desvinculaciones.
- ✅ Menor carga operativa para soporte TI
- ✅ Auditoría y cumplimiento normativo
- ✅ Compatible con MFA y políticas corporativas

·buk·

Protege tu acceso, protege la información

Hola, mi nombre es María y soy la administradora de la plataforma.
María sabe que **no debe compartir su usuario ni su contraseña de Buk**, porque cada cuenta contiene información privada y sensible.

Un día, José le pidió su contraseña y, aunque María sabía que no debía hacerlo, decidió **prestarle su acceso**.

Esto puede **provocar alteraciones en la plataforma**, errores en los datos y afectar la seguridad de la información.

No seas como María: **protege tus credenciales y cuida la información de la plataforma**.

Historial de Cambios

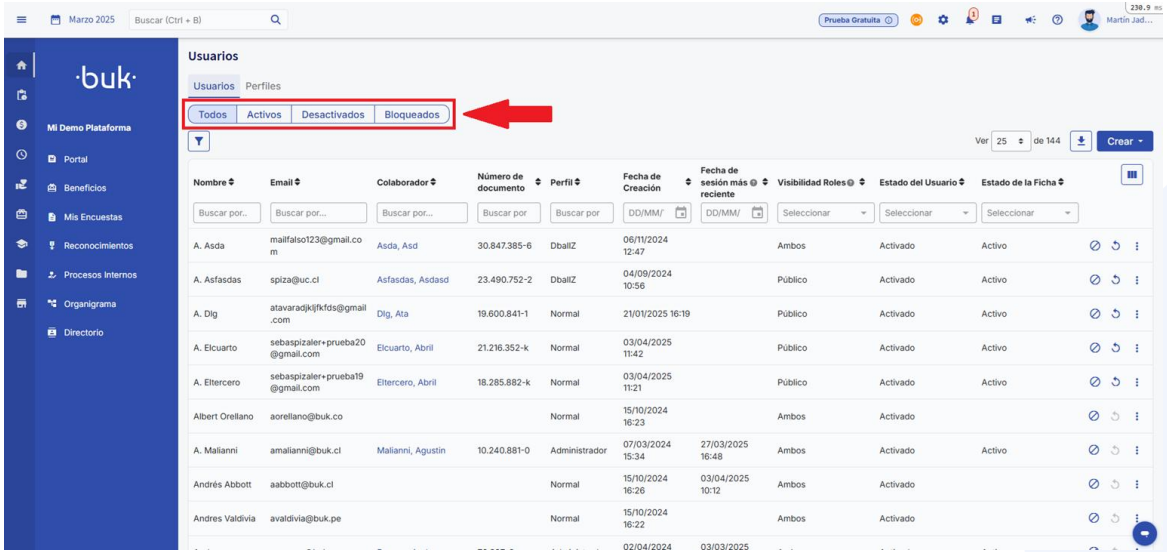
Revisa todas las modificaciones realizadas dentro de la plataforma. Esto contempla la creación, actualización y eliminación de cualquier ítem, documento, solicitud, encuesta, usuario, etc. En resumen, todo cambio que realice algún usuario administrador de Buk.

Historial de Cambios

David Diaz (Administrador)	Diaz, Mariana F1	1.012.404.861	Persona (35)	Modificar	27/08/2025 09:35:17	Email	Prueba123445@gmail.com
David Diaz (Administrador)	Diaz, Mariana F1	1.012.404.861	Persona (35)	Modificar	27/08/2025 09:35:17	Teléfono Particular	3007876629
David Diaz (Administrador)	Diaz, Mariana F1	1.012.404.861	Persona (35)	Modificar	27/08/2025 09:35:17	Teléfono Oficina	31348129
David Diaz (Administrador)	Diaz, Mariana F1	1.012.404.861	Persona (35)	Modificar	27/08/2025 09:35:17	rut_uncasted	
David Diaz (Administrador)	Diaz, Mariana Marisol Real F1	1.012.404.861	Usuario (18)	Modificar	27/08/2025 09:35:17	Email	prueba123445@gmail.com

Usuarios y Perfiles

Gestionar correctamente los usuarios: crear y vincular usuarios, activar o desactivar accesos, editar configuraciones de usuario, visualizar información relevante y facilitar la activación inicial de las cuentas.



Activación de usuario
- Individualmente
- Por Grupo
- Normal a Todos

Perfiles
- Creación de perfiles
- Personalizar Perfiles
- Configurar perfil normal

Material de Apoyo

Configurar reCAPTCHA en Buk

Es una herramienta avanzada que protege los sitios web detectando si una acción está siendo realizada por una persona real o por un bot. Analiza el comportamiento del usuario y otros factores para tomar decisiones en tiempo real. Si detecta actividad sospechosa, puede bloquear el acceso o presentar un desafío (por ejemplo, seleccionar imágenes) para verificar que se trata de un humano. Esto permite proteger la plataforma sin interrumpir la experiencia de los usuarios legítimos.

⚠️ Evaluación adaptativa del riesgo

✅ Detección avanzada de bots

🎓 Aprendizaje continuo

Material de Apoyo

📌 Importante: El reCAPTCHA no aparece siempre, sino sólo en los casos donde el sistema detecta un posible intento de acceso indebido. Esta evaluación es automática y se basa en múltiples factores de riesgo.

Restablecer Contraseña

Aprenderás a realizar el proceso de restablecimiento de contraseña dentro de la plataforma.

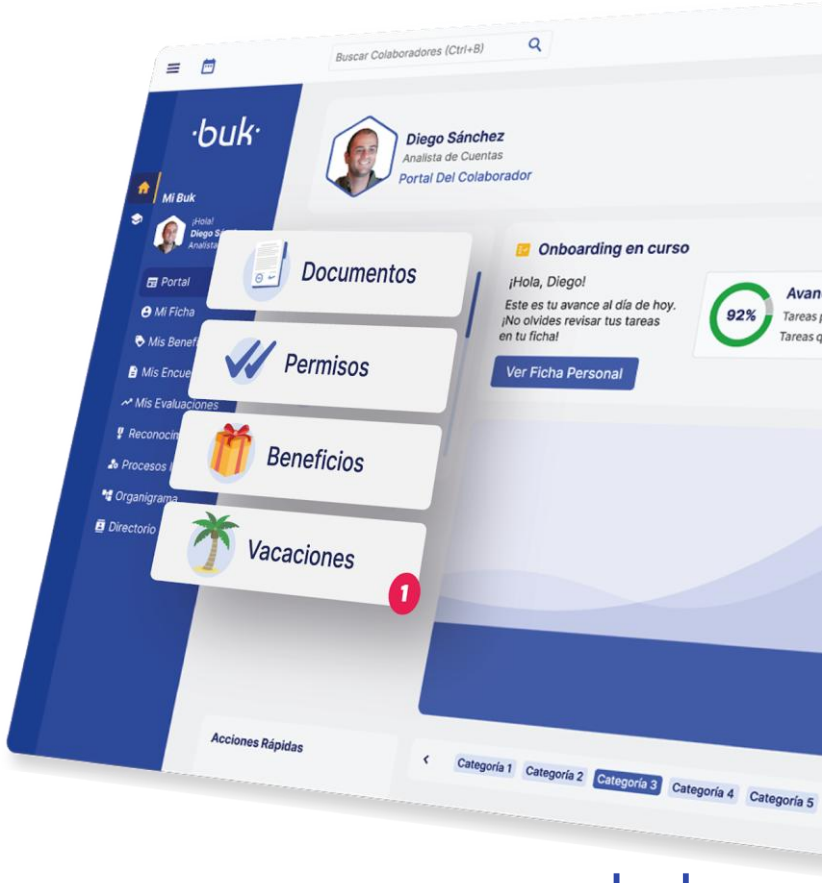
Este procedimiento es fundamental para garantizar el acceso seguro y continuo a tus herramientas de trabajo. A través de unos pasos sencillos, podrás generar una nueva contraseña en caso de olvido o pérdida de la anterior, asegurando que tu información se mantenga protegida y que puedas retomar tus actividades sin contratiempos.

- Restablecimiento por correo electrónico
- Restablecimiento por SMS

Material de Apoyo

¿Como configurar todo esto en Buk?

Vamos a la plataforma…



buk

Crea un lugar de trabajo **más feliz ;)**

buk Gestión de **Personas**