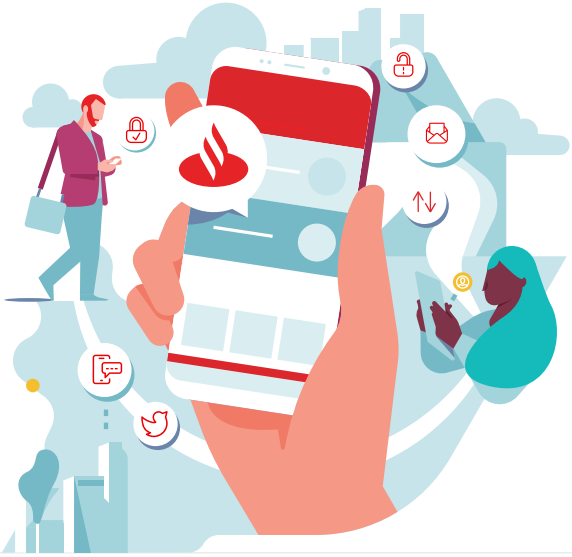
5 Ciber principios para proteger tu negocio

Prácticos y sencillos consejos para ayudarte a proteger tu negocio en el contexto digital actual.



1 Protege tu información y tu equipo

- **Mantén el software actualizado:** Ordenadores, teléfonos móviles... asegúrate de que sus programas, antivirus y aplicaciones están siempre al día. Sus actualizaciones suelen incluir importantes parches de seguridad, así que prográmalas para que se hagan de forma automática y no te pierdas nada.
- **Protege tu website con HTTPS:** La 'S' es de seguridad, lo que te permitirá encriptar automáticamente la información que entre y salga de tu web, protegiendo tus datos y generando confianza con tus clientes.
- **Haz copias de seguridad regularmente:** Protege tu negocio haciendo copias de seguridad de la información necesaria para el buen funcionamiento del día a día. Cuanto más crítica sea la información, más a menudo deben hacerse las copias. Asegúrate de tener una que no éste en la red, en caso de que las otras se viesen comprometidas.

2 Sé discreto online y en publico

- **Consulta la huella digital de tu negocio:** Utiliza buscadores online para ver lo que puedes encontrar sobre él en la red. Recuerda, no reveles más de lo necesario. Si la información acaba en malas manos, puede ser aprovechada con fines fraudulentos.
- **Define público frente a privado:** Entender que información se puede compartir externamente, hará más fácil para todos el protegerla y manejarla de forma segura.
- **Conciencia sobre las responsabilidades:** Los empleados son un activo clave de tu negocio por lo que es importante que les ayudes a entender el impacto directo de que puede tener el compartir información externamente, ya sea en redes sociales o con terceros.

3

Piensa antes de hacer clic o responder

- **Atento no solo a los emails:** El phishing puede ocurrir por correo electrónico, llamada telefónica, SMS o mensajería instantánea. Asegúrate de que todos los empleados saben cómo detectar comunicaciones sospechosas.
- **Conoce las amenazas:** Existen ataques dirigidos específicamente a empresas en los que se hacen pasar por un superior o un proveedor para convencerte que hagas un pago.
- **Protege a los demás:** Dificulta el que puedan hacerse pasar por tu negocio y engañar a tus clientes o proveedores. Mantén tus comunicaciones consistentes y personalizadas y si estás pensando en hacer cambios, comunícalos con anticipación.

4

Mantén tus contraseñas seguras

- **Usa el múltiple factor de autentificación (MFA):** Con el MFA añades una capa adicional de seguridad. Puede consistir en un código enviado a tu móvil, tu huella dactilar o reconocimiento facial. Úsalo siempre que sea posible e intenta ofrecerlo en tus plataformas.
- **Promueve el uso de contraseñas resistentes:** Las contraseñas siempre deben ser fuertes y nunca compartirse ni re-usarse. Los `passphrases´, tres o más palabras consecutivas, son una buena opción y además fáciles de recordar.
- **Cambia contraseñas predeterminadas:** Muchos dispositivos vienen por defecto con contraseñas de fábrica, que son fáciles de identificar. Cámbialas antes de empezar a utilizarlos.

5

Si sospechas, repórtalo

- **Define procesos y canales de reporte:** Establece una forma sencilla y accesible de reportar incidentes de ciber para empleados, proveedores y clientes.
- **Fomenta una cultura de ciberseguridad:** Es importante que los empleados se sientan cómodos y sepan qué hacer ante este tipo de incidentes.
- **Considera tu cadena de suministro:** Puede ocurrir que quien sufra un ciber incidente sea uno de tus proveedores. Asegúrate que cuentan con un proceso para avisarte y que puedas actuar con rapidez.

Los empleados son la primera linea de defensa de tu negocio. Comparte con ellos estos principios.

Santander