

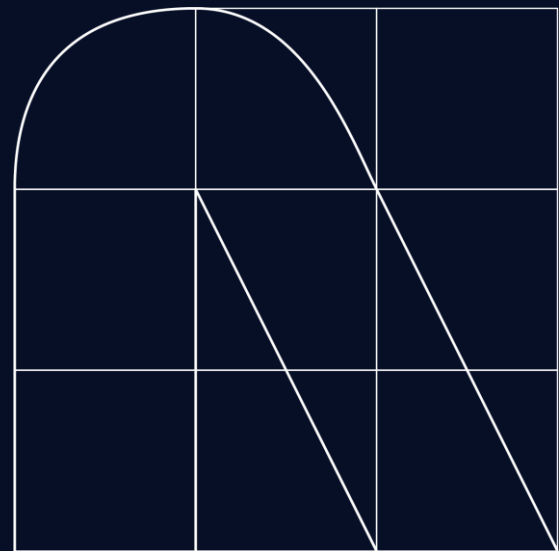


Octubre · Mes de la Ciberseguridad

7 hábitos para una vida digital más segura

Guía breve para convertir buenas decisiones digitales en hábitos cotidianos.

La seguridad empieza en cada decisión



La ciberseguridad también es una cuestión de hábitos

Pequeñas decisiones cotidianas pueden marcar una gran diferencia.

ANTES DE EMPEZAR

La seguridad empieza en cada decisión. No hace falta ser especialista en ciberseguridad para reducir el riesgo. Muchas de las decisiones que protegen nuestra información, nuestra identidad y nuestra organización empiezan en acciones sencillas que repetimos cada día.

Las amenazas evolucionan, las herramientas cambian y la inteligencia artificial hace que algunos engaños sean cada vez más convincentes. Pero una parte importante de la seguridad sigue dependiendo de decisiones muy humanas: detenerse antes de hacer clic, comprobar una petición inesperada, proteger una identidad o avisar cuando algo no encaja.

Esta guía reúne siete hábitos sencillos para empleados y ciudadanos. No buscan convertirlos en expertos, sino ayudarles a desarrollar un mejor criterio digital y a reaccionar de forma más segura ante situaciones cotidianas.

LOS 7 HÁBITOS, DE UN VISTAZO

- 01 Piensa antes de hacer clic.
- 02 Protege tu identidad digital.
- 03 Verifica antes de confiar.
- 04 Comparte solo lo necesario.
- 05 Mantén tu entorno digital al día.
- 06 Ante la duda, reporta.
- 07 Entrena continuamente tu criterio digital.



Frena el impulso. Protege el acceso

Dos hábitos básicos para reducir riesgos antes de que se conviertan en incidentes.

01

Piensa antes de hacer clic

Muchos engaños digitales buscan provocar una reacción inmediata: urgencia, miedo, curiosidad o la sensación de que debemos actuar antes de pensar. Un correo, un mensaje o un enlace puede parecer rutinario y, precisamente por eso, resultar convincente.

El hábito más útil es introducir una pequeña pausa. Antes de abrir un archivo, seguir un enlace o responder a una petición inesperada, observa el contexto: ¿esperabas ese mensaje?, ¿el remitente es realmente quien dice ser?, ¿te pide algo inusual? Unos segundos de comprobación pueden evitar una decisión difícil de revertir.



PONLO EN PRÁCTICA

Pausa unos segundos y comprueba remitente, contexto y petición antes de actuar.

02

Protege tu identidad digital

En el entorno digital, nuestras credenciales representan quiénes somos y qué podemos hacer. Por eso, proteger una cuenta no consiste solo en elegir una contraseña difícil: significa reducir las posibilidades de que otra persona pueda hacerse pasar por nosotros.

Utiliza contraseñas diferentes para servicios distintos, activa la autenticación multifactor siempre que esté disponible y evita compartir códigos de acceso, incluso cuando la petición parezca venir de alguien conocido. En el trabajo, sigue los mecanismos oficiales para solicitar o conceder permisos. La identidad es una puerta de entrada; cuanto mejor la protejamos, más difícil será convertir una credencial comprometida en un incidente mayor.



PONLO EN PRÁCTICA

Activa MFA y no compartas contraseñas, códigos ni accesos por canales no oficiales.



Una pausa a tiempo y una identidad bien protegida son dos de las decisiones más sencillas -y más eficaces- que podemos convertir en hábito.

Verifica. Comparte con criterio

La confianza digital se construye comprobando antes de actuar y reduciendo la exposición innecesaria.

03

Verifica antes de confiar

La inteligencia artificial puede hacer que un mensaje, una voz o una imagen parezcan muy convincentes. Por eso, una de las competencias digitales más importantes es separar apariencia y confianza: que algo “parezca real” ya no es suficiente para considerarlo auténtico.

Cuando recibas una petición poco habitual relacionada con dinero, datos sensibles, cambios de acceso o información confidencial, verifica por un segundo canal. Una llamada al número que ya conoces, un mensaje por el canal corporativo o una comprobación directa pueden ser suficientes. La verificación no es desconfianza; es una forma responsable de proteger a las personas y a la organización.



PONLO EN PRÁCTICA

Para peticiones sensibles o inusuales, confirma siempre por un segundo canal conocido.

04

Comparte solo lo necesario

La seguridad también depende de cuánto exponemos. Cada documento, dato, permiso o conversación compartida amplía el número de personas y sistemas que deben proteger esa información. Aplicar el principio de “solo lo necesario” reduce el riesgo sin complicar el trabajo.

Antes de enviar un archivo, publicar información o conceder acceso, pregúntate quién necesita realmente verla y durante cuánto tiempo. Evita trasladar datos sensibles a canales no autorizados y revisa destinatarios antes de pulsar “enviar”. En el ámbito personal ocurre lo mismo: cuanto más publicamos sobre rutinas, viajes, trabajo o relaciones, más contexto ofrecemos a quienes intentan construir engaños creíbles.



PONLO EN PRÁCTICA

Revisa destinatarios, permisos y canal antes de compartir información o archivos.

Mantén tu entorno preparado y avisa rápido

Actualizar y reportar son hábitos de prevención y respuesta, no tareas exclusivamente técnicas.

05

Mantén tu entorno digital al día

Actualizar no es solo incorporar nuevas funciones. Las actualizaciones corrigen errores y vulnerabilidades que pueden ser aprovechados por atacantes. Posponerlas indefinidamente puede dejar abierta una puerta que ya sabemos cómo cerrar.

Convierte la actualización en una rutina: aplica las actualizaciones de sistemas y aplicaciones cuando corresponda, reinicia los dispositivos cuando sea necesario y evita instalar software desde fuentes no confiables. En entornos corporativos, respeta las políticas de actualización de la organización y no intentes desactivar controles porque resulten incómodos. Un entorno digital cuidado es menos vulnerable y también más fácil de proteger.



PONLO EN PRÁCTICA

Actualiza cuando corresponda y usa únicamente software y canales autorizados.

06

Ante la duda, reporta

Un mensaje sospechoso, un acceso extraño o incluso un clic accidental no deberían ocultarse. Cuanto antes conozca una organización una posible incidencia, más opciones tendrá para analizarla, contenerla y reducir su impacto.

Reportar no significa estar seguro de que existe un ataque. Significa compartir una señal para que pueda ser evaluada. Si has abierto un archivo dudoso, introducido una contraseña donde no debías o detectado un comportamiento extraño, utiliza cuanto antes el canal definido por tu organización. En el ámbito personal, cambia credenciales cuando sea necesario y contacta con el servicio afectado por sus canales oficiales.



PONLO EN PRÁCTICA

Si algo no encaja, comunícalo rápido. Una alerta temprana puede reducir el impacto.

Entrena tu criterio digital

La cultura de seguridad se construye cuando aprender deja de ser puntual y se convierte en una práctica continua.



07

Entrena continuamente tu criterio digital

Las amenazas cambian porque también cambian la tecnología, los canales y nuestros propios hábitos. Una formación realizada una vez al año puede ayudar, pero la verdadera cultura de seguridad se construye cuando aprendemos de forma continua y aplicamos ese aprendizaje a situaciones reales.

Participa en las formaciones, simulaciones y comunicaciones de seguridad que tengas disponibles. Presta atención a nuevos tipos de fraude y comparte aprendizajes con compañeros, familiares o personas que puedan tener menos experiencia digital. El objetivo no es vivir en alerta permanente, sino reconocer patrones, hacer mejores preguntas y saber qué hacer cuando aparece una situación inesperada.



PONLO EN PRÁCTICA

Revisa periódicamente tus hábitos y comparte lo aprendido con tu entorno.



7 HÁBITOS, UNA MISMA IDEA

No hace falta ser experto en ciberseguridad para tomar mejores decisiones de seguridad.

Hace falta convertirlas en hábitos: parar, verificar, proteger, compartir con criterio, actualizar, reportar y seguir aprendiendo.

La seguridad empieza en cada decisión

Conoce cómo NTT DATA puede ayudarte a fomentar una cultura de seguridad a través de formación continua y experiencias de aprendizaje adaptadas a tu organización.



Contacta con grupo.hacking@nttdata.com para información sobre Formación y Concientización en Ciberseguridad.

