



# Memorias

## ¿Cómo prevenir un fraude digital en transacciones internacionales?

Grupo Bancolombia  
2020

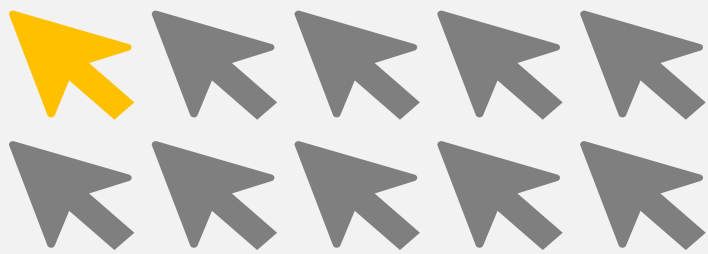
VIGILADO SUPERINTENDENCIA FINANCIERA DE COLOMBIA BANCOLOMBIA S.A. Establecimiento Bancario

VIGILADO SUPERINTENDENCIA FINANCIERA DE COLOMBIA

VIGILADO

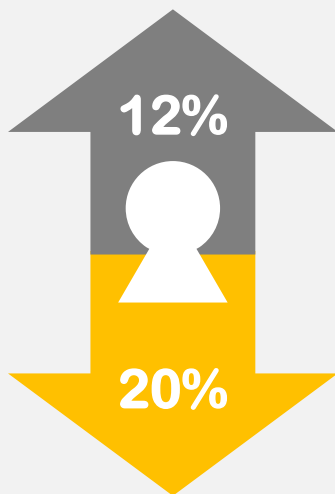


# CONTEXTO DE AMENAZAS



**1** DE CADA **10** URL  
ES MALICIOSA

**RANSOMWARE  
EN EMPRESAS**



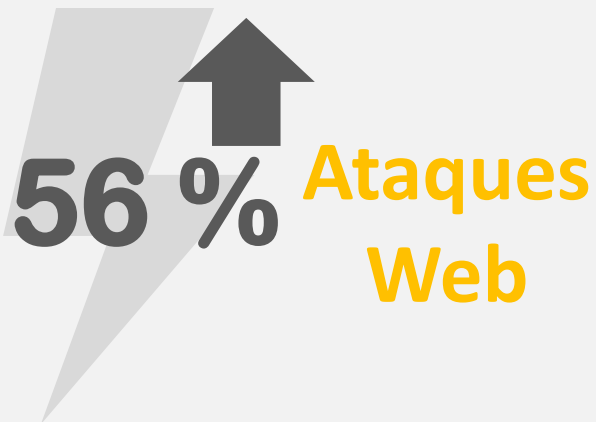
**RANSOMWARE  
EN GENERAL**



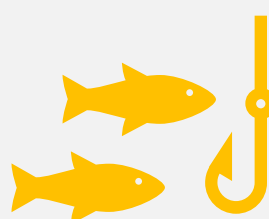
**27.4%** PROMEDIO AÑO  
AUMENTO ANUAL DE  
BRECHAS DE SEGURIDAD



**48%**  
ADJUNTOS  
MALICIOSOS EN  
EMAIL: OFFICE



**90%**  
ATAQUES POR CORREO  
ELECTRÓNICO



**91%**  
ATAQUES POR  
PHISHING

# AMENAZAS CIBERNÉTICAS



¿Cuáles son las más recurrentes?

## Ingeniería social



Conjunto de diversas técnicas usadas por los defraudadores para lograr obtener la información de sus víctimas y luego, usar esos datos para robar el dinero o cometer otro tipo de fraude.

## Spear Phishing

Es una variante de phishing, en la que mediante correos de una fuente supuestamente confiable, recolectan la información de la víctima, y luego la redirigen a un sitio web falso con malware.



## Malware



Envío de archivos maliciosos o "virus" por medio de adjuntos a través de correos electrónicos para infectar los equipos y capturar la información.

## Ransomware 2.0

Secuestro de la información de la compañía y posibles amenazas de publicar los datos que ha extraído ilegalmente de forma cifrada.

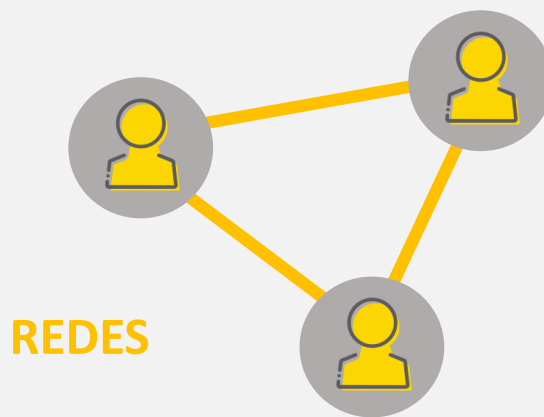


# ¿Cómo protegerse?

## Desde la tecnología



Una estrategia de protección frente al panorama de amenazas cibernéticas, debe tener el respaldo total de la alta dirección y no se resuelve únicamente con mejoramiento o implementación de controles tecnológicos, aunque son importantes, la estrategia debe ser integral, para tomar acciones no solo desde la Tecnología, sino también desde los procesos y las personas.



Este se refiere a los controles de protección y respuesta transversales a la organización que buscan interceptar, examinar y bloquear de ser necesarios, accesos no permitidos por posibles intentos de ataque.

**Control de correo electrónico:** dado que esta es una de las vías más usadas por los delincuentes debemos fortalecer las medidas de contención y filtrado en aspectos como correo SPAM, links y anexos maliciosos y suplantación o robo de las cuentas de correo, es decir, contar con un mecanismo de protección ante un intento de robo de una cuenta.

**Control de navegación:** Busca dar visibilidad y control sobre que sitios se pueden navegar desde los equipos corporativos, implementando el concepto de listas negra para bloquear sitios ya publicados como de alto riesgo y evitar así, el ingreso a páginas redireccionadas desde correo u otros sitios web.

**Firewall:** Puede ser corporativo, de pc o ambos, este nos permite bloquear intentos de ingreso no permitidos a la organización o al dispositivo.

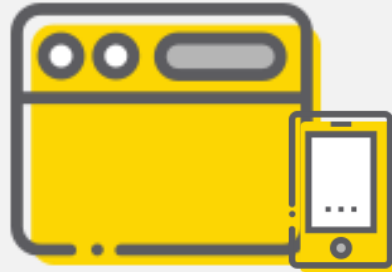


# ¿Cómo protegerse?

## Desde la tecnología



### DISPOSITIVOS



Se refiere a los mecanismos de protección implementados en las estaciones de trabajo, dispositivos como smartphones y tablets que permitan la interacción con la organización.

#### Controles en el Sistema Operativo:

- Mantener actualizado el sistema operativo de los dispositivos, no solo en versión, también en parches de seguridad y funcionalidad.
- Definir una base de configuración del sistema operativo que permita reforzarlo para evitar ataques, ejemplos: deshabilitar protocolos o funciones de riesgo que no sean necesarias.
- Limitar el uso de usuarios administradores en equipos y el de puertos USB, este último puede ser la puerta para el ingreso de un malware a la organización o fuga de información confidencial

- **Antivirus**

Aunque tenerlo no necesariamente evita un ataque, no tenerlo deja muy vulnerable los dispositivos.

- Se debe contar con un antivirus licenciado.
- Mantener rutinas de actualización de Firmas y versiones de este.
- Contar con complementos que ya ofrecen los nuevos antivirus como detección y bloqueo por comportamiento, protección para navegación y uso de correo entre otros.



# ¿Cómo protegerse?

## Desde la tecnología



### IDENTIDAD



La identidad es la llave de acceso a las aplicaciones e información de la organización, por eso el robo de datos es una motivación constante para los delincuentes.

- **Contraseñas fuertes** : Definir lineamientos que guíen y exijan a los usuarios que sus contraseñas sean creadas con niveles de complejidad media o alta con aspectos como longitud, caracteres especiales, mayúsculas y números. Se deben evitar palabras comunes como meses del año, nombres de personas, nombres de la compañía o áreas.
- **Mínimos privilegios** : Definir claramente que accesos se debe dar en aplicaciones e información a cada persona de la organización según su rol y responsabilidad, ni más ni menos; evitar así dar accesos innecesarios que pongan en riesgo la organización.
- **Doble Factor de autenticación**: Con el fin de robustecer el proceso de autenticación se han implementado diferentes métodos de validación adicionales al usuario y contraseña, este segundo factor se puede implementar de diversas formas, como un mensaje de correo que debe ser aprobado, un app del celular que debe aprobar ciertas condiciones y el método más antiguo, un token que cambia una clave cada cierto tiempo.

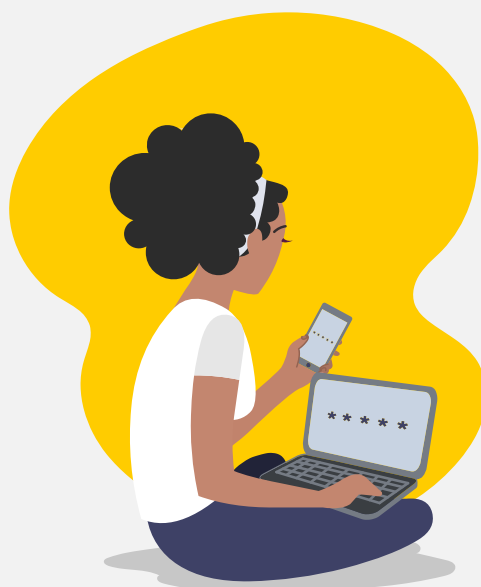
Por último, en este aspecto, no se recomienda usar la misma contraseña personal para los accesos corporativos y en caso de manejar diferentes accesos, no debe repetir la misma contraseña en todos.



# ¿Cómo protegerse?

## Desde las personas

En el ámbito de las personas desde la ciberseguridad “El eslabón más débil, es el ser humano”, esto se refiere a que en seguridad no hay elementos que garanticen seguridad al 100% para nuestras organizaciones y llegará algún momento de verdad donde nuestros colaboradores se enfrentarán a una decisión frente a un correo, una página web, un mensaje o pantalla de navegación e incluso una llamada, por esta razón se deben dar herramientas y definir modelos de actuación que faciliten tomar la mejor decisión minimizando el riesgo al que pueden estar expuesto.



**“ Para la seguridad digital el factor humano es el eslabón más débil”**

## COMPROMISO DE TODOS



Formación para los empleados sobre seguridad.



Acciones de sensibilización y concienciación en seguridad.



Medición constante del cumplimiento de las buenas prácticas en seguridad.



Definición y divulgación de políticas, comportamientos y procedimientos de seguridad.



# ¿Cómo protegerse?

## Desde los procesos



### CONOCIMIENTO Y AUTENTICACION DEL PROVEEDOR / INTERMEDIARIO

¿Es el proveedor una entidad establecida con un historial comercial verificable?

¿El proveedor “genuino” no está siendo suplantado?

¿El proveedor me direcciona a un intermediario?

### NEGOCIACIÓN Y COMPRA



¿Precio/cantidad ofrecidos son razonables y en línea con circunstancia actual de mercado?

¿El proveedor ha proporcionado detalles sobre los productos, su origen, cómo se envían y la ruta?

¿El contrato incluye terminología inusual?  
¿El proveedor me impone urgencia o exige un pago anticipado “sustancial”?









# ¿Cómo protegerse?

## Desde los procesos



### AL MOMENTO DEL PAGO



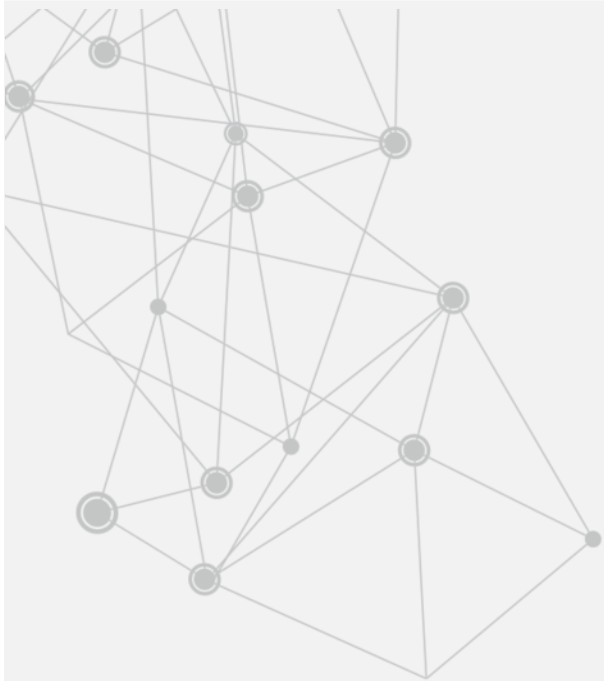
-  Establezca protocolos de pago con límites y niveles de aprobación
-  Siempre confirme verbalmente instrucciones de pago a nuevos beneficiarios o cuando un proveedor establecido “cambie” la cuenta
-  Examine cuidadosamente el remitente cuando la instrucción de pago sea vía Email
-  Mantenerse alerta cuando correo mencione: Urgente – Confidencial - Secreto
-  Establezca procedimientos o controles para pagos a “Nuevos Beneficiarios” o pagos fuera del estándar.
-  No ceda ante la presión y cuestione/sospeche en cualquier solicitud fuera de lo habitual



# Respondemos sus inquietudes

Establezca procedimientos o controles para pagos a “Nuevos Beneficiarios” o pagos fuera del estándar.





**Esperamos que  
este contenido  
aporte a la  
seguridad de  
su empresa.**

