Solaria

TÍTULO: **PROCEDIMIENTO DE PREVENCIÓN DEL FRAUDE**
CÓDIGO DE DOCUMENTO: **Protocolo corporativo de prevención del fraude**

Nº REVISIÓN:	01	**DOCUMENTO EMITIDO PARA:**	Coordinación de departamentos
FECHA EMISIÓN:	06/07/2026		

SCM	ERM	DLC
Preparado por:	**Revisado por:**	**Aprobado por:**

RESUMEN DE REVISIONES

Revisión	Fecha	Descripción de los cambios
01	06/07/2026	Documento nuevo

ÍNDICE

1. OBJETO.

Establecer las medidas de prevención, verificación y respuesta ante intentos de fraude basados en la suplantación de identidad de directivos, responsables de departamento, proveedores o clientes con el fin de obtener pagos fraudulentos o información confidencial.

2. ALCANCE.

Este procedimiento es de obligado cumplimiento para:

- Todo el personal de la empresa.
- Becarios.
- Colaboradores externos.
- Proveedores con acceso a sistemas o información corporativa.

Y especialmente, para la:

- Dirección General.
- Departamento Financiero.
- Compras.
- Recursos Humanos.
- Personal con capacidad para autorizar pagos o acceder a información sensible.

Aplica a todos los dispositivos y sistemas utilizados para el desempeño de actividades profesionales, tanto corporativos como personales cuando estén autorizados para acceder a recursos de la empresa.

El incumplimiento de este procedimiento podrá ser considerado una infracción de las normas internas de seguridad y dará lugar a la adopción de las medidas organizativas y disciplinarias que resulten de aplicación, sin perjuicio de las responsabilidades legales que pudieran derivarse.

2.1. Definiciones.

Phishing.

El phishing es un intento de engañar a un usuario para que revele información confidencial (contraseñas, códigos de verificación, datos bancarios, etc.) o instale software malicioso, haciéndose pasar por una persona o entidad de confianza.

Los ataques pueden llegar por:

- Correo electrónico.
- Mensajes SMS (smishing).
- WhatsApp o aplicaciones de mensajería.
- Llamadas telefónicas (vishing).
- Redes sociales.

Cómo identificar un posible phishing

Desconfíe si el mensaje presenta alguna de estas características:

- Solicita contraseñas, información confidencial o códigos de verificación.
- Procede de un remitente desconocido o de una dirección casi igual a la de un remitente habitual.
- Pide realizar una transferencia o un pago urgente.
- Contiene errores ortográficos o de redacción.
- Incluye enlaces sospechosos o acortados.
- Contiene archivos adjuntos inesperados.
- Genera sensación de urgencia (p. ej. "su cuenta será bloqueada").

2.2. Responsabilidades.

Todos los empleados son responsables de:

- Cumplir este procedimiento.
- Actuar con prudencia ante cualquier comunicación sospechosa.
- Proteger sus credenciales.
- Notificar inmediatamente cualquier incidente o sospecha.

Departamento de Seguridad, es responsable de:

- Gestionar los incidentes comunicados.
- Analizar los correos o mensajes sospechosos.
- Coordinar las acciones de respuesta.
- Informar a la Dirección cuando proceda.
- Promover campañas de concienciación.

3. RIESGOS CUBIERTOS.

Este protocolo contempla, entre otros:

- Suplantación del CEO o de los directores generales.
- Suplantación de responsables de departamentos.
- Cambio fraudulento de cuentas bancarias de proveedores o empleados.
- Solicitudes urgentes de transferencia.
- Facturas falsas.

- Robo de credenciales.
- Solicitudes de información financiera o fiscal.
- Fraude mediante llamadas telefónicas o videollamadas.

4. PRINCIPIO GENERAL.

Ningún directivo o responsable de departamento de Solaria está autorizado a:

- Solicitar pagos urgentes sin seguir el procedimiento establecido.
- Pedir confidencialidad sobre operaciones económicas.
- Solicitar credenciales o códigos.
- Ordenar cambios de cuentas bancarias únicamente por correo electrónico.

5. PROCEDIMIENTO DE VERIFICACIÓN OBLIGATORIA.

Toda solicitud relacionada con:

- transferencias,
- pagos extraordinarios,
- modificaciones o cambios de cuenta bancaria,
- modificación de datos de proveedores,
- pagos internacionales,
- compra urgente de tarjetas regalo o vales,
- envío de información financiera,

deberá verificarse mediante un segundo canal independiente. Se consideran canales válidos:

- llamada telefónica a un número ya registrado,
- reunión presencial,
- videollamada corporativa,
- plataforma interna autorizada.

Nunca se utilizarán los datos de contacto incluidos en el propio correo sospechoso.

Nunca se autorizarán cambios basados únicamente en un correo electrónico.

6. INDICADORES DE FRAUDE.

Considere sospechosa cualquier solicitud que incluya:

- urgencia inusual,
- petición de confidencialidad,
- presión para actuar inmediatamente,

- solicitudes inusuales de superiores o directivos,
- cambios inesperados de procedimientos habituales,
- cuentas bancarias nuevas,
- errores ortográficos, gramaticales o de redacción,
- remitentes desconocidos,
- dominios distintos pero muy similares al corporativo,
- enlaces acortados,
- horarios poco habituales,
- instrucciones para evitar controles internos.

La existencia de uno solo de estos indicadores obliga a detener el proceso y verificar la autenticidad de la solicitud.

7. ACTUACIÓN ANTE UNA SOSPECHA.

7.1. Normas generales de seguridad.

Mantenga actualizado su equipo y teléfono móvil con las últimas actualizaciones.

Si algo parece extraño, consulte antes de actuar.

Mantenga una actitud de desconfianza razonable ante cualquier solicitud inesperada.

Todos los empleados de Solaria deberán cumplir las siguientes normas:

7.2. Verificación del remitente. Antes de responder a cualquier comunicación:

- Verificar la dirección completa del remitente.
- Confirmar que el dominio pertenece realmente a la organización emisora.
- Desconfiar de direcciones con pequeñas variaciones ortográficas.

7.3. Verificación de enlaces. Antes de acceder a un enlace:

- Comprobar el destino real del enlace situando el cursor sobre él.
- Acceder preferentemente escribiendo la dirección web en el navegador.
- No utilizar enlaces enviados por terceros cuando exista otra forma de acceso.

7.4. Archivos adjuntos. No deberán abrirse archivos adjuntos cuando:

- No se estuvieran esperando.
- Procedan de remitentes desconocidos.

- Presenten extensiones ejecutables o inusuales.
- Generen cualquier duda sobre su legitimidad.

7.5. Credenciales. Queda terminantemente prohibido:

- Introducir sus credenciales desde un enlace recibido por correo.
- Compartir contraseñas.
- Enviar credenciales por correo electrónico.
- Facilitar contraseñas por teléfono, correo o mensajería.
- Autorizar solicitudes de autenticación que no hayan sido iniciadas por el propio usuario.
- Bloquee su equipo cuando se ausente del puesto de trabajo.

7.6. Solicitudes económicas Toda solicitud relacionada con:

- transferencias,
- modificaciones de cuentas bancarias,
- pagos extraordinarios o urgentes,
- compras urgentes,
- cambio de datos de proveedores,

deberá verificarse mediante un canal independiente (llamada telefónica al número de teléfono utilizado para contactar habitualmente, reunión presencial, Teams o canal corporativo previamente establecido).

No se autorizarán cambios basados únicamente en un correo electrónico.

Si existe cualquier duda:

1. Suspenda inmediatamente el proceso.
2. No ejecute el pago.
3. No responda al correo.
4. No hacer clic en enlaces ni abrir archivos adjuntos.
5. Contacte directamente con el supuesto remitente mediante un canal válido independiente como los que se señalan anteriormente.
6. Informe al Departamento de Seguridad.
7. Conservar el mensaje hasta recibir instrucciones.

8. PRINCIPIO DE PROTECCIÓN DEL EMPLEADO.

Ningún trabajador será penalizado por detener una operación económica cuando existan dudas razonables sobre su legitimidad y actúe de buena fe siguiendo este procedimiento.

La organización prioriza la verificación de las operaciones frente a la rapidez en su ejecución.

REGLA CORPORATIVA: "VERIFICAR ANTES DE PAGAR"

NINGUNA URGENCIA COMERCIAL, PETICIÓN DE UN DIRECTIVO O SOLICITUD DE UN PROVEEDOR JUSTIFICA OMITIR LOS CONTROLES DE SEGURIDAD ESTABLECIDOS POR LA ORGANIZACIÓN.

ANEXO I. LISTA RÁPIDA DE COMPROBACIÓN

Antes de actuar, pregúntese:

☐ ¿Conozco al remitente?

☐ ¿Esperaba este correo o mensaje?

☐ ¿Solicita información confidencial?

☐ ¿Pide actuar con urgencia?

☐ ¿El enlace lleva realmente al sitio oficial?

☐ ¿Solicita aprobar una autenticación?

☐ ¿He verificado la solicitud por otro canal?

Si alguna respuesta genera dudas, **no actúe y comunique la incidencia al Departamento de Seguridad**.

ANEXO II. DECÁLOGO CORPORATIVO CONTRA EL PHISHING

La seguridad de la información depende de todos

1. Desconfíe de lo inesperado

Si recibe un correo, mensaje o llamada que no esperaba, verifique siempre su autenticidad antes de actuar.

2. Compruebe quién envía el mensaje

No se fíe únicamente del nombre del remitente. Revise la dirección de correo completa y confirme que pertenece al dominio oficial de la organización.

3. No haga clic impulsivamente

Antes de acceder a un enlace, sitúe el cursor sobre él para comprobar su destino. Si tiene dudas, escriba manualmente la dirección web en el navegador.

4. No abra archivos adjuntos sospechosos

No abra documentos ni archivos ejecutables que no espere recibir o cuya procedencia no pueda verificar.

5. Nunca facilite sus credenciales

La empresa, los proveedores tecnológicos, los bancos o los organismos públicos nunca solicitarán sus contraseñas o códigos de autenticación por correo electrónico, teléfono o mensajería.

6. Verifique siempre las solicitudes de pago

Toda petición de transferencia, cambio de cuenta bancaria o modificación de datos financieros deberá confirmarse mediante un canal independiente previamente establecido.

7. No apruebe autenticaciones que no haya iniciado

Si recibe una solicitud de autenticación multifactor (MFA) sin haber iniciado sesión, rechácela e informe inmediatamente al Departamento de Seguridad.

8. Mantenga la calma ante mensajes urgentes

Los ciberdelincuentes utilizan la urgencia, el miedo o la autoridad para provocar decisiones precipitadas. Deténgase, analice la situación y confirme la solicitud.

9. Comunique cualquier sospecha

Ante la mínima duda, informe al Departamento de Seguridad. Es preferible comunicar una falsa alarma que no detectar un incidente real.

10. Recuerde la regla de oro

PARE – PIENSE – VERIFIQUE – ACTÚE

Si una comunicación solicita información confidencial, dinero o credenciales, no actúe hasta haber verificado su legitimidad.