Seguridad de la Información

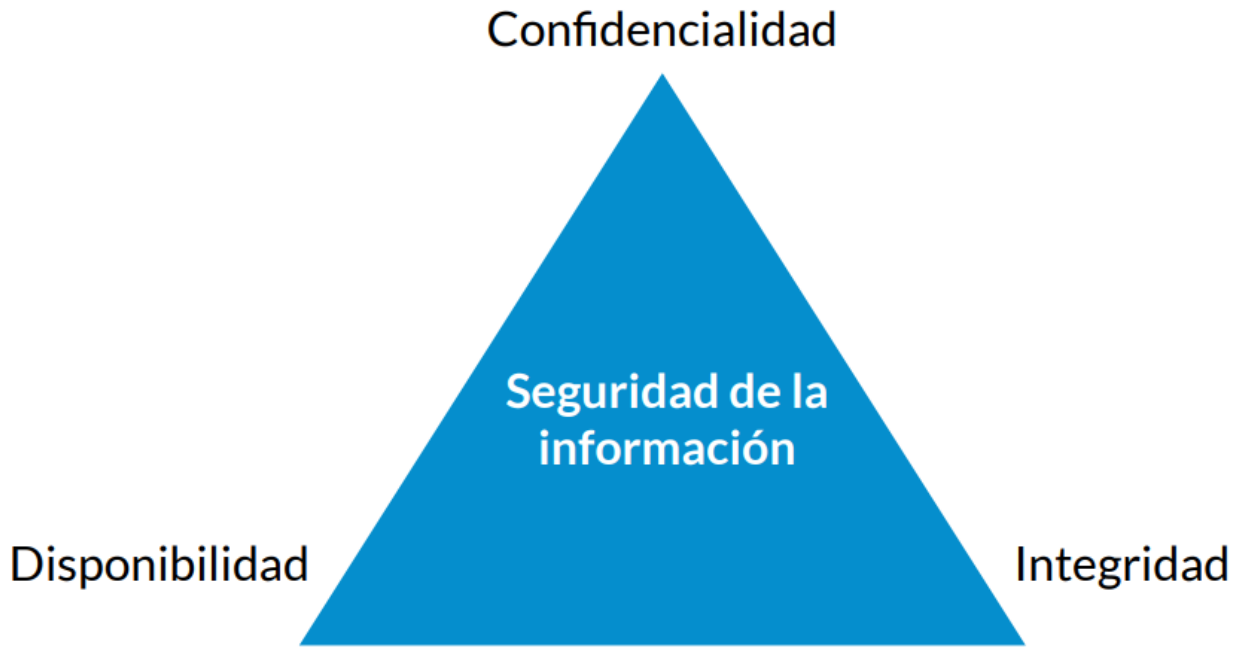
OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN
Y LAS COMUNICACIONES | OTIC

ALCALDÍA MAYOR DE BOGOTÁ D.C.
DEPARTAMENTO ADMINISTRATIVO DEL SERVICIO CIVIL DISTRITAL
BOGOTÁ

Fuente: *pmg-ssi.com*

Seguridad de la Información:

Conjunto de medidas preventivas de las organizaciones y sistemas tecnológicos con el objetivo de proteger la **información**.



¿A qué estamos expuestos?

Malware

- Virus (gusanos, troyanos, keyloggers, etc.)
- Spyware
- Phishing
- Ransomware
- Ingeniería social

Vulnerabilidades

- Contraseñas
- Usuarios

Fuente: *osi.es*

Fuente: *Instituto Nacional de Ciberseguridad - España*

Ransomware

Malware enfocado a la extorsión, bloquea acceso a la información o a un dispositivo a cambio del pago de un rescate, generalmente en un determinado plazo.

Efectos:
- Pérdida temporal o permanente de la información.
- Interrupción de actividades.
- Pérdidas económicas o de reputación.

Medidas de protección:
- Conocer políticas de seguridad de la información:
- Uso permitido de aplicaciones y dispositivos.
- Seguridad en el puesto de trabajo.
- Política de contraseñas.

Ingeniería social

Esta es la práctica de manipular personas *(persuasión y convencimiento)* para obtener información confidencial sin que el objetivo se percate.

Las personas somos el eslabón más débil en cuanto a seguridad informática se refiere…

Elementos:

- Confianza (Prestos a ayudar, difícil decir "no", nos gusta que nos alaben)
- Distracción.
- Atención selectiva.

*"El **80%** de los ataques informáticos se deben a errores relacionados con el factor humano y no a temas específicos de tecnología.'*

Ingeniería social

Ejemplos:

* **Phishing** → Mensajes por e-mail que aparentan ser confiables.

* **Vishing** → Phishing por voz.

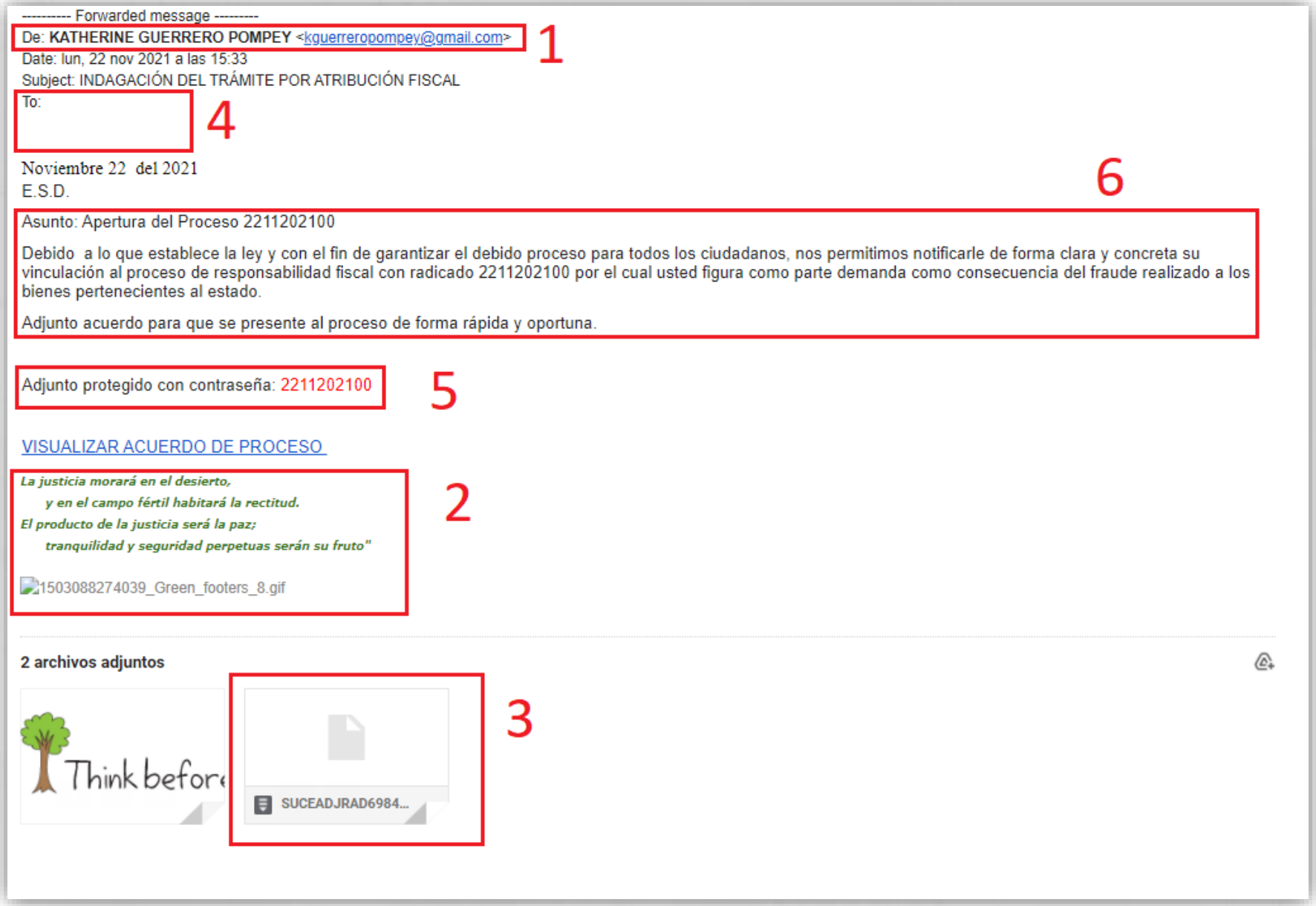
* **Smishing** → Phishing por SMS.

* **Pretexting** → suplantación de identidad.

Medidas de prevención:

- Aprender a decir NO
- Cuando no se esté seguro de una respuesta, responder con una pregunta.
- No hacer clic en vínculos sospechosos.
- Escritorio limpio (contraseñas)
- **Bloqueo de dispositivos en ausencia.**

#DejamosHuellaEnElServicioCivil



---------- Forwarded message ---------
De: **KATHERINE GUERRERO POMPEY** <kguerreropompey@gmail.com> 1
Date: lun, 22 nov 2021 a las 15:33
Subject: INDAGACIÓN DEL TRÁMITE POR ATRIBUCIÓN FISCAL
To: 4

Noviembre 22 del 2021
E.S.D.

6

Asunto: Apertura del Proceso 2211202100

Debido a lo que establece la ley y con el fin de garantizar el debido proceso para todos los ciudadanos, nos permitimos notificarle de forma clara y concreta su vinculación al proceso de responsabilidad fiscal con radicado 2211202100 por el cual usted figura como parte demanda como consecuencia del fraude realizado a los bienes pertenecientes al estado.

Adjunto acuerdo para que se presente al proceso de forma rápida y oportuna.

Adjunto protegido con contraseña: 2211202100 5

VISUALIZAR ACUERDO DE PROCESO

La justicia morará en el desierto,
y en el campo fértil habitará la rectitud.
El producto de la justicia será la paz;
tranquilidad y seguridad perpetuas serán su fruto"

1503088274039_Green_footers_8.gif 2

2 archivos adjuntos

Think before

SUCEADJRAD6984... 3

PHISHING

Cómo indentificarlo:

1. **Remitente**; correo informal.
2. **Firma**; no institucional.
3. **Adjunto**; archivo sospechoso.
4. **Destinatario**; información que no es clara.
5. **Contraseña**; algo inusual
6. **Aviso**; temas de urgencia para generar miedo.

Caso INVIMA

Desde el pasado 06 de febrero las plataformas tecnológicas dispuestas por esta entidad dejaron de operar, esto ha causado el represamiento de contenedores con alimentos y medicamentos y otros productos.

*__Proceso registro e inspección__

Sistema → **De manera manual**

2h → **36h** (promedio)

Implicaciones:

*Pérdida de información

*Pérdidas económicas

*Alzas en el precio de productos

Causa:

Ransomware Blackbyte

Que, en relación con lo anterior y atendiendo la contingencia referida, la Oficina de Tecnologías de la Información advirtió a la Dirección General sobre la imposibilidad de acceder a los siguientes servicios desde el 6 de febrero de 2022:

- Correos electrónicos
- Carpetas compartidas
- Información almacenada en los equipos PC
- Acceso a aplicativos utilizados por las misionales y los procesos de apoyo

Indicando que se observa una afectación en las actividades que se desarrollan en la misionalidad del Invima y que requieren del uso de tecnologías de la información.

Fuente: *Resolución 2022500001 del 15 de febrero de 2022*

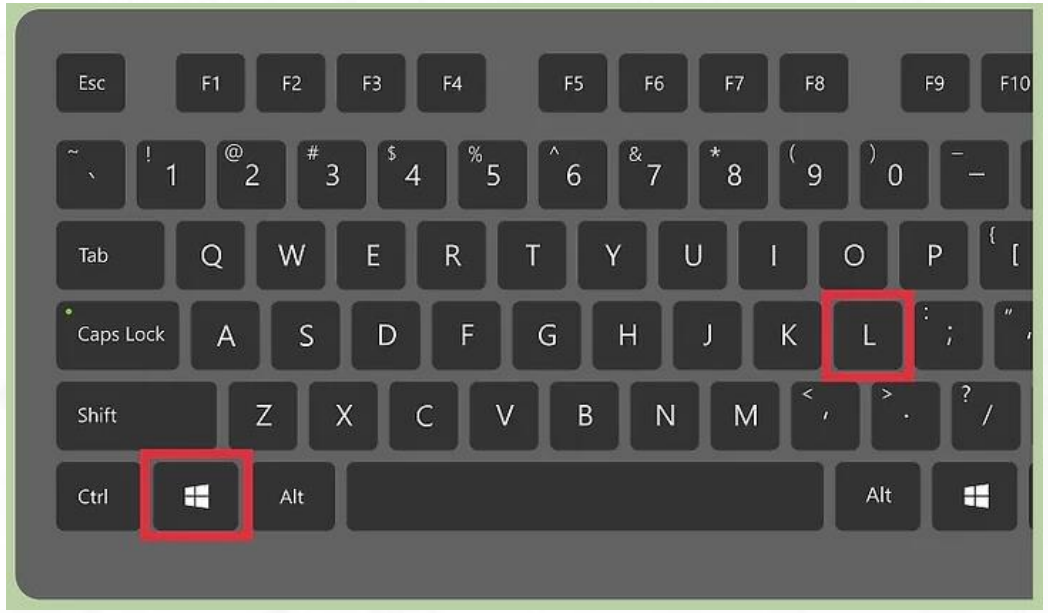
Pérdidas semanales por $15.000 millones en puerto de Buenaventura deja ciberataque al Invima

Cerca de 3.000 contenedores de medicamentos, alimentos y cosméticos están varados en el Puerto de Buenaventura.

18/2/2022

Fuente: *semana.com*

Fuente: *invima.gov.co*



Fuente: *wikihow.com*

Fuente: *haycanal.com*

Ajuste de Política de Seguridad GPO

* ***Actualización sobre el proceso de cambio de contraseñas***

- Reducción sobre el tiempo de bloqueo de pantalla (inactividad)
  15 minutos → **10** minutos

- Es importante realizar cambio de contraseña periódicamente, de acuerdo a la política establecida, las contraseñas deben actualizarse cada 3 meses.

- Si no se realiza este cambio, el sistema bloquea automáticamente al usuario → *Se debe crear caso por la mesa de ayuda para realizar este desbloqueo*.

A-TIC-IN-004 INSTRUCTIVO CAMBIO DE CONTRASEÑA USUARIO FINAL V2.0

Mapa de procesos → Procesos de apoyo a la gestión → Gestión de TIC's → Guías, instructivos, protocolos TI.

2. POLÍTICAS DE SEGURIDAD EN CONTRASEÑAS

Dentro de las políticas de seguridad de contraseñas implementadas en el DASCD, se contemplan las siguientes condiciones:

- ✔ Usar letras mayúsculas y minúsculas: ABCDefgh
- ✔ Usar números: 1234567890
- ✔ Usar caracteres especiales: ¡"#$%&/()=?¡
- ✔ Longitud mínima: 8 caracteres
- ✔ Debe ser diferente a las anteriores: Últimas diez (10) contraseñas utilizadas
- ✔ Se solicitará cambio frecuente: Cada 120 días
- ✔ Se dará notificación de cambio: Últimos cinco días antes de vencer
- ✔ La contraseña no debe contener nombres ni apellidos propios del usuario
- ✔ El usuario se bloquea después de 5 intentos de ingreso fallidos
- ✔ Se solicitará ingreso de contraseña para desbloqueo de pantalla transcurridos 10 minutos de inactividad en los equipos de cómputo de los funcionarios del DASCD.

E-SIN-MA-001 MANUAL DE LA ESTRATEGIA DE SEGURIDAD DIGITAL V2

Mapa de procesos → Estratégicos Direccionamiento Institucional → Seguridad de la información → Manuales, planes, Doc Estratégicos SI.

11.2. POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA

El personal del DASCD debe conservar su escritorio libre de información propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.

El personal del DASCD debe bloquear la pantalla de su computador, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo.

Al imprimir documentos de carácter confidencial, estos deben ser retirados de la impresora inmediatamente.

Cuando no se esté usando información sensible o crítica para la entidad se deberá asegurar bajo llave u otro medio y protegerla de acceso no autorizado.

Las sesiones de usuario se deben cerrar y proteger con contraseña cuando el usuario se ausente en forma temporal o por largos períodos de tiempo

Al finalizar sus actividades los usuarios deben verificar que en sus puestos de trabajo no quede expuesta información crítica o sensible para la entidad.

Los usuarios son responsables y asumen las consecuencias de la perdida de información que esté bajo su custodia.

Los usuarios deben concientizarse de ahorro del consumo de energía y uso racional, apagando el computador y dispositivos electrónicos a su cargo una vez termine la jornada de trabajo

La OTIC es la responsable de verificar el cumplimiento de esta política en todos los equipos de cómputo que hay en la entidad.

GRACIAS!

OTIC