UNIVERSIDAD ORT
Uruguay

01/06/2023

UTILIZACIÓN Y SOPORTE DE RECURSOS INFORMÁTICOS

DOCUMENTO N.º 600

1) INTRODUCCIÓN

Los recursos informáticos puestos a disposición de los funcionarios deben utilizarse adecuadamente, con responsabilidad y según los lineamientos previstos en el presente documento y los que la universidad informe oportunamente.

El uso indebido de los recursos informáticos puede afectar negativamente el funcionamiento de los equipos de oficina (PC), la red, los servidores y hasta la imagen de la universidad.

Todo el personal de la Universidad ORT Uruguay tiene acceso a una serie de recursos informáticos, a saber:

a) Datos y programas residentes en los equipos centrales de la universidad.

b) Paquetes de software distribuido (residentes en el equipo ubicado en la oficina asignada, en salones de clase o salas docentes) que contribuyen con su tarea.

c) Apoyo directo del Departamento de Servicios Informáticos (DSI) para la utilización de los recursos mencionados en los puntos anteriores.

Es importante resaltar que:

a) Los recursos se asignan según las funciones y responsabilidades de cada usuario dentro de la universidad.

b) La universidad es la dueña de los datos, programas, procesos y software de base (tanto a nivel centralizado como distribuido) antes mencionados y será considerada como falta grave el retirar de la universidad cualquiera de estos elementos o copia de ellos sin la autorización escrita correspondiente de la dirección de la Universidad ORT Uruguay o de quien esta disponga. Ello sin perjuicio de las consecuencias y/o sanciones previstas por la normativa legal vigente.

Queda expresamente prohibida la reproducción o cualquier otra forma o procedimiento de explotación de los recursos informáticos de la universidad por parte del personal o de aquellos que, sin ser funcionarios o docentes de la universidad, tengan derecho para su uso.

Sin perjuicio de lo establecido en el presente artículo, quien viole la presente disposición será personalmente responsable de dicho incumplimiento y se obliga a mantener indemne a la universidad en caso de existir cualquier reclamo vinculado a dicha conducta.

Asimismo, se dispone expresamente que todos los datos e información contenidos en los recursos informáticos son propiedad de la universidad y, en consecuencia, queda prohibido cualquier manejo para fines no académicos o administrativos sin la debida autorización escrita correspondiente de la Dirección o de quien esta disponga.

Cualquier incumplimiento a lo dispuesto precedentemente será considerado una falta grave, ello sin perjuicio de las consecuencias y/o sanciones previstas por la normativa legal vigente.

Los equipos asignados solo pueden ser utilizados por el usuario designado para las funciones y responsabilidades asignadas dentro de la universidad. Las tareas de *service* y mantenimiento deben ser realizadas por personal expresamente designado por DSI.

DSI realizará auditorías periódicas del software existente en las computadoras asignadas, siendo el usuario el único responsable de la existencia de software sin licencia y de las consecuencias que ello conlleve.

El presente documento detalla los diferentes tipos de recursos informáticos disponibles, la manera de acceder a ellos y su debido tratamiento. Esto sin perjuicio de otra reglamentación interna que pueda dictar la universidad para el tratamiento de casos o dispositivos específicos, u otros que, producto de los avances tecnológicos, requieran de un tratamiento inmediato y para lo cual dicha reglamentación será debidamente comunicada.

2) INSTALACIÓN DE SOFTWARE

La universidad solo utiliza software original.

Para utilizar software el usuario administrativo debe enviar una solicitud de instalación a DSI (mediante el sistema de solicitudes a DSI).

Esta solicitud es evaluada por el vicerrector académico, quien autoriza o no la instalación de acuerdo con las licencias compradas y los estándares fijados.

Si el software deseado no ha sido autorizado, el usuario debe enviar un pedido de evaluación al Comité Técnico de Software, que estudiará la factibilidad y los costos.

Si el Comité Técnico aprueba la compra, se debe solicitar la autorización de compra al encargado del área que requiere la compra.

La universidad no se responsabiliza por la utilización de software obtenido por cualquier otra vía, prohibiendo toda violación a los derechos de propiedad, en conformidad con la normativa legal vigente.

Los usuarios deben informar a DSI cualquier tipo de situación, irregularidad o evento referente a la violación de las disposiciones legales sobre adquisiciones o reproducción de software.

DSI dará a los usuarios administrativos mantenimiento y asesoramiento solamente para el software registrado en el catálogo.

El software existente en las computadoras de usuarios administrativos solo puede ser actualizado por personal de DSI una vez que el usuario haya hecho la solicitud correspondiente (mediante el sistema de solicitudes a DSI).

Los docentes deben canalizar sus pedidos a través del coordinador de su área.

3) VIRUS Y CÓDIGOS MALICIOSOS

Es responsabilidad del usuario salvaguardar la información de su computadora asignada contra virus informáticos y otros códigos maliciosos.

Para este fin DSI, a través del área de Soporte, instala en cada equipo asignado un programa antivirus que se actualiza de forma centralizada cada vez que el usuario encienda su computadora. No se debe interferir con la operación del antivirus.

El usuario debe utilizar únicamente aquel software original, dispositivos USB, CD, DVD o cualquier otro soporte de almacenamiento de información que haya sido previamente analizado por el detector de virus.

Cualquier problema que surja durante la ejecución del detector de virus debe comunicarse a DSI en forma inmediata.

De todas maneras, y frente a cualquier duda o irregularidad en el funcionamiento de su computadora, el usuario debe consultar de forma inmediata a DSI.

El usuario se encuentra obligado a:

a) Verificar (según la reglamentación interna que dicte la universidad) su cuenta de correo electrónico a efectos de velar por la integridad del sistema y evitar cualquier tipo de exposición innecesaria a contaminación de virus informáticos.

b) Escanear de forma completa y periódica la computadora asignada, recomendándose un escaneo semanal.

DSI auditará periódicamente las computadoras asignadas y el usuario será el responsable de la infección, si la hubiera, y de sus consecuencias.

4) RESPALDOS

Es responsabilidad del usuario respaldar periódicamente su información, ya sea a dispositivos USB, DVD, disco duro externo u otro almacenamiento brindado por ORT.

DSI diseñará procedimientos y brindará capacitación cuando sea necesario.

En ciertos casos, cuando la información sea considerada vital para la universidad, DSI se encargará de auditar los respaldos, a pedido del decano o director del área.

En cualquiera de los casos, el usuario es el responsable directo de la ejecución y el estado de los respaldos, la frecuencia del respaldo y la selección de la información respaldada.

5) ACCESO A DATOS, SERVICIOS, PROGRAMAS Y CORREO ELECTRÓNICO

Cada usuario administrativo tiene un nombre de usuario (*username*) que lo identifica, y una contraseña (*password*) que le permite acceder a los datos y procesos habilitados.

El área de Recursos Humanos de la universidad es la única autorizada para solicitar altas, bajas y modificaciones de usuarios administrativos.

También es la que informa el perfil de seguridad de los usuarios administrativos, lo que determina cuáles son los datos y procesos a los que pueden acceder.

En cuanto a los perfiles de usuarios en las computadoras de los usuarios administrativos, solamente el personal de DSI está autorizado a crearlos.

El acceso a datos, servicios y programas es privado de cada usuario.

La contraseña es secreta y privada. Por tanto, no debe ser conocida por otra persona.

Ante cualquier tipo de duda de que la contraseña haya dejado de ser privada, el usuario debe modificarla de inmediato.

Toda acción registrada con una determinada contraseña será asumida como efectuada por el usuario propietario de la misma.

Por razones de seguridad, y aunque el sistema o programa utilizado no requiera el cambio periódico de la contraseña para su uso, se recomienda que el usuario modifique su contraseña cada 90 días.

La contraseña debe ser fácil de recordar, de manera que no haya que escribirla o guardarla en un archivo en el equipo.

Es conveniente elegir una contraseña que:

- Tenga doce o más caracteres.
- Combine mayúsculas, minúsculas y números.
- No figure, o tenga probabilidad de figurar, en un diccionario.
- Sea difícil de adivinar (se debe evitar el uso de nombres de parejas, hijos, mascotas, matrículas de vehículos, fechas de nacimiento, códigos postales, entre otros).

6) HARDWARE

El usuario del equipamiento informático que se le ha asignado es el único responsable directo de preservar la seguridad y el estado de este.

El coordinador del área de Soporte de DSI es el único autorizado para decidir sobre la recepción, entrega y movimientos de equipos.

Además del personal de DSI, solo está habilitado a mover equipos el personal de Servicios Físicos, pero únicamente en aquellos casos en que el coordinador del área de Soporte de DSI se lo solicite expresamente y por escrito.

El incumplimiento de los puntos anteriores será considerado una falta grave.

Cada usuario es responsable de notificar (a través del sistema de solicitudes a DSI) si su equipo presenta alguna falla en el funcionamiento. DSI se encargará de llamar al servicio técnico.

Cada coordinador de cursos es responsable de notificar (a través del sistema de solicitudes a DSI) si los equipos de las salas docentes presentan alguna falla en el funcionamiento. DSI se encargará de llamar al servicio técnico.

En ninguna circunstancia el usuario podrá proceder a su reparación en forma individual.

Cuando un usuario administrativo necesite adquirir nuevo equipamiento informático, debe enviar una solicitud de compra a DSI (mediante el sistema de solicitudes a DSI) y el área se encargará de adquirirlo.

Cada usuario administrativo es responsable de que las etiquetas de inventario que cada equipo tiene pegadas estén en buen estado de conservación y con los datos correctos.

Cada coordinador de cursos es responsable de que las etiquetas de inventario que cada equipo de las salas docentes tiene pegadas estén en buen estado de conservación y con los datos correctos.

Cambios de denominación de oficinas

Si se requiere una nueva etiqueta o actualizar los datos de esta, se debe notificar a través del sistema de solicitudes a DSI.

DSI se encargará de actualizar los datos e imprimir y colocar la nueva etiqueta.

7) INFORMACIÓN RESIDENTE EN LAS COMPUTADORAS ASIGNADAS

Cada usuario es responsable de la información residente en la computadora que le sea asignada.

Si posee información confidencial debe:

- Encriptarla.
- Proteger el acceso al equipo y a la sesión de usuario del sistema operativo.
- Protegerla físicamente (mantenerla en CD, DVD, disco duro externo o dispositivo USB bajo llave) y borrarla.

Además, es responsabilidad de cada usuario cerciorarse si está compartiendo el disco de su computadora o alguna carpeta con otros usuarios, y habilitarlo o no cuando lo crea conveniente. En principio se recomienda no compartir el acceso al equipo.

Los archivos, mensajes o datos que sean de índole personal (es decir, que no atañen a las funciones y responsabilidades derivadas de la actividad desarrollada por el usuario) no deben almacenarse en los equipos de la universidad.

La institución tiene el derecho de acceder y auditar el efectivo cumplimiento de esta obligación. Y, en caso de detectar información de índole personal, virus o necesitar espacio disponible, previa comunicación, la información podrá ser borrada.

A partir de la fecha de desvinculación del funcionario con la institución, este ya no tendrá más derecho de acceso al equipo asignado ni a la información allí residente, ya que la misma será considerada información no personal y será objeto de eliminación.

8) USO DEL CORREO ELECTRÓNICO

La utilización de la casilla de correo electrónico asignada al usuario (en dominio ort.edu.uy), está sujeta a las siguientes condiciones:

- Los usuarios solo pueden utilizar el correo electrónico para recibir y/o enviar correspondencia inherente a sus tareas.

- Los usuarios no tienen ningún derecho personal por ningún objeto creado, recibido o enviado a través de su casilla de correo. La universidad se reserva el derecho de auditar cualquier objeto creado, recibido y/o enviado que transite por redes de la Universidad ORT Uruguay o que se haya originado o recibido en usuarios y equipos de la institución, incluyendo aquellos equipos localizados en espacios de la universidad que sean de uso exclusivo de funcionarios o docentes.

- No se debe tener, por parte de quien usa el correo electrónico, expectativas de privacidad debido a que se usen contraseñas u otras medidas de seguridad.

- El usuario tiene prohibido crear o enviar mensajes que puedan constituir material intimidatorio, hostil u ofensivo sobre la base del sexo, raza, color, religión, orientación sexual, discapacidad o cualquier otro aspecto que pueda ser lesivo para la moral o las buenas costumbres.

Cualquier incumplimiento de los puntos anteriores se considerará una falta grave.

El usuario no está obligado a responder o enviar correos electrónicos, ni a realizar cualquier otro tipo de comunicación como ser llamadas, mensajes de texto, mensajes de WhatsApp, etc, fuera del horario de trabajo establecido. La única excepción admitida es en caso de solicitud por escrito de su superior directo.

A partir del momento mismo de la desvinculación del funcionario con la institución, este no tendrá más derecho a acceder a la casilla de correo electrónico provista por la universidad.

9) ACCESO A LA RED

Solo el personal de DSI está autorizado para conectar una computadora a la red de datos, exceptuándose las redes inalámbricas internas de acceso público.

10) USO DE INTERNET

La navegación en Internet debe ser autorizada por el decano o director del área.

La navegación en Internet debe ser realizada en forma responsable y para fines vinculados a la actividad que se desarrolla en la universidad.

Por razones de seguridad interna, la navegación queda registrada y puede ser controlada por la universidad.

Dada la posibilidad de usar la tecnología informática con fines ilegítimos y/o delictivos, en la medida que sea necesario la universidad regulará e informará sobre aquellos procedimientos tendientes a minimizar cualquier tipo de riesgo para la institución y sus sistemas que se deriven de la navegación por Internet. Los usuarios quedan obligados a aceptar dichos procedimientos.

Está prohibido el uso de Internet para fines que violen las reglamentaciones vigentes de la universidad, incluyendo, entre otros, la transmisión y/o descarga de material obsceno o pornográfico, que contenga amenazas o cualquier tipo de información que atente contra la moral o las buenas costumbres.

La infracción a esta disposición será considerada una falta grave.

11) HORARIOS DE APOYO AL USUARIO

Dentro del marco expuesto en este documento, DSI brinda apoyo:

En relación con servidores:	De 8:00 a 23:00
En relación con computadoras asignadas:	De 8:00 a 21:00

ANEXO 1 – CONTRASEÑAS: CÓMO ELEGIRLAS Y CAMBIARLAS

La contraseña debe ser fácil de recordar, de manera que no haya que escribirla o guardarla en un archivo en el equipo.

Cómo elegirlas

Es conveniente elegir una contraseña que:

- Tenga doce o más caracteres.
- Combine mayúsculas, minúsculas y números.
- No figure, o tenga probabilidad de figurar, en un diccionario.
- Sea difícil de adivinar (evitar el uso de nombres de parejas, hijos, mascotas, matrículas de vehículos, fechas de nacimiento, códigos postales, entre otros).

Es conveniente usar una frase en vez de una palabra, ya que es más difícil de adivinar.

Cuando se manejan diferentes sistemas que requieren una contraseña para cada uno, nunca hay que repetir la misma contraseña para diferentes sistemas.

Tampoco se deben usar contraseñas "recicladas", que tienen pequeños cambios para cada sistema (por ejemplo, "usuario1" para el sistema 1 y "usuario2" para el sistema 2).

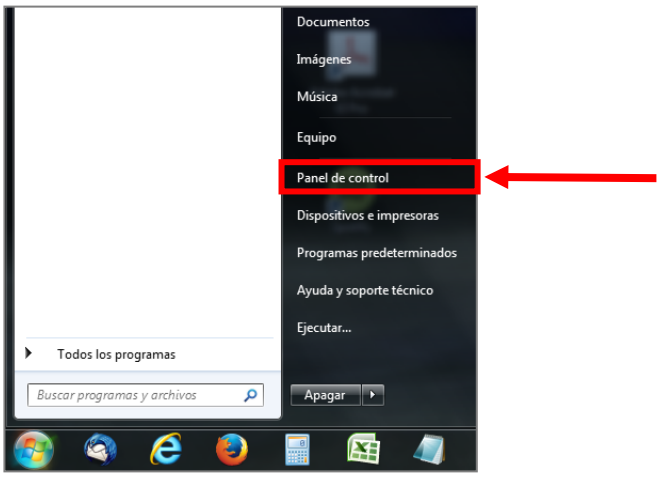
No se debe revelar la contraseña a nadie, ni tampoco escribirla ni tenerla registrada en ninguna parte más que en la memoria del usuario.

Algunos sistemas de la Universidad ORT Uruguay obligan al cambio periódico de contraseña. En cambio, la contraseña asignada inicialmente en la universidad debe ser cambiada por el usuario en Windows y en el correo electrónico.

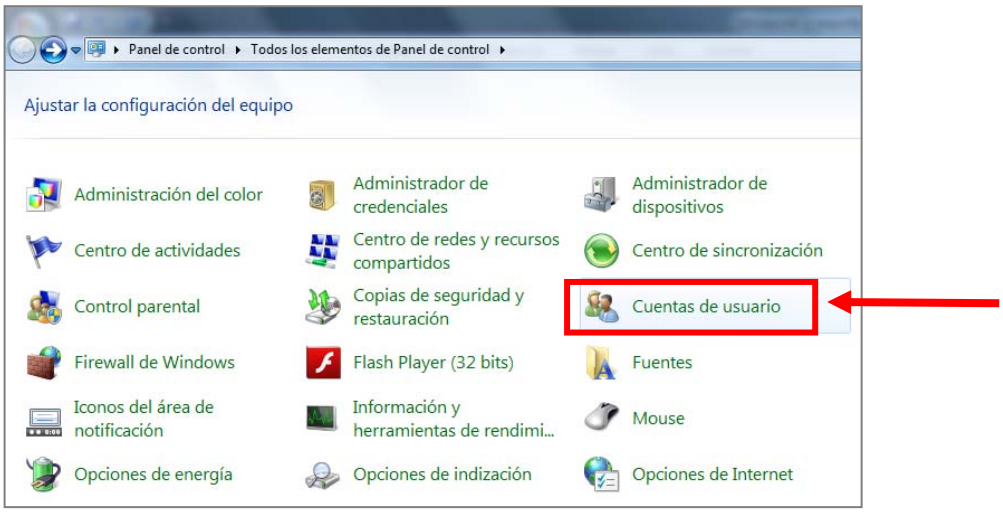
Dónde cambiar la contraseña del equipo

Para cambiar la contraseña en Windows 7 se debe ir a:

1) Inicio
2) Panel de control



3) Ingresar en “Cuentas de usuario”



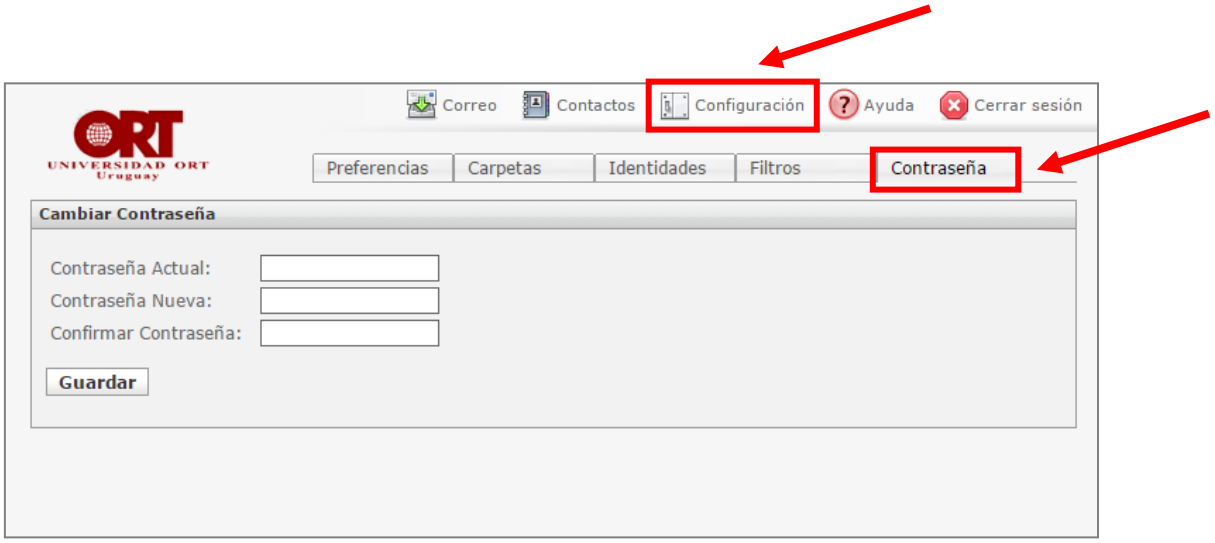
4) Elegir la cuenta propia
5) Luego hacer clic en “Cambiar la contraseña”

Dónde cambiar la contraseña del correo electrónico

La contraseña del correo electrónico se modifica a través del webmail.

Para ello:

1) Desde el navegador, ingresar a: http://webmail.ort.edu.uy
2) Ir a “Configuración”.
3) Luego ir a la pestaña “Contraseña”.
4) Allí ingresar la contraseña actual y luego, dos veces, la nueva.



Luego de cambiar la contraseña se recomienda reiniciar el equipo para que las unidades de red que pudieran estar conectadas se actualicen y tomen la nueva contraseña.

En caso de dudas, por favor consultar a DSI.

ANEXO 2 – DISPOSITIVOS USB Y VIRUS

Riesgos de los dispositivos USB

Los dispositivos de almacenamiento siempre constituyeron una de las vías más comunes de infección, desde los viejos discos magnéticos de 5 1/4, pasando por los ya casi olvidados disquetes de 3 y 1/2, hasta llegar a los dispositivos de almacenamiento que permiten guardar información a través del puerto USB.

Los medios de almacenamiento masivo a través de conexiones del tipo USB, como los *pendrives* (también conocidos como *flashdrives* o memorias USB) representan un punto vulnerable para cualquier sistema informático.

Por su diseño, estos dispositivos pueden cargar automáticamente programas a la computadora cuando se conectan. Por su masividad de uso y facilidad de conexión, se convierten en un medio común utilizado para transportar archivos y también todo tipo de virus.

Cuando se usan estos dispositivos es recomendable respetar mínimas medidas de protección, como verificar con una herramienta antivirus los dispositivos que se conecten a la computadora, para asegurar que se encuentran libres de códigos maliciosos.

Cómo chequear virus

Todas las computadoras de la Universidad ORT Uruguay tienen instalado el programa antivirus contratado por la institución.

El antivirus chequea exclusivamente los archivos sensibles a infección, como, por ejemplo: exe, com, pif y bat, entre otros. Y prácticamente no recarga el funcionamiento del equipo.

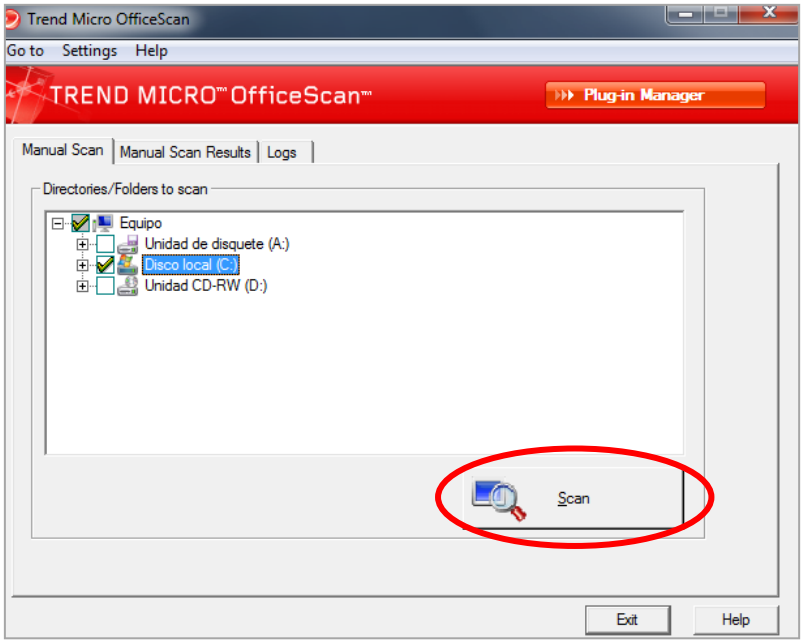
Para verificar que tenemos instalado el antivirus, observar la barra de tareas de Windows: abajo a la derecha se encuentra el ícono correspondiente (a la izquierda de la hora y la fecha).

Es conveniente escanear nuestro equipo con el antivirus periódicamente, para asegurarnos de no tener ningún virus. Podemos escanear un único archivo que seleccionemos, una carpeta, una unidad o todas las unidades de almacenamiento.

Para realizar un escaneo de todo el sistema (todas las unidades de nuestra computadora) se debe hacer clic en el botón derecho del ratón sobre el ícono del antivirus de la barra de tareas y seleccionar la opción “OfficeScan Console”.

Se abrirá la aplicación TREND MICRO OfficeScan. Seleccionar las unidades a escanear haciendo clic en el botón izquierdo del ratón sobre las diferentes unidades, para marcar las casillas deseadas.

Una vez seleccionadas las unidades, el escaneo comienza haciendo clic en el botón izquierdo del ratón sobre el botón “Scan”.



El escaneo proporciona mensajes en caso de encontrar virus.

Si no se comprenden los mensajes o se tienen dudas sobre el estado del equipo, es importante consultar a DSI cuanto antes.

ANEXO 3 – EL PHISHING Y SUS CONSECUENCIAS

Hay mafias organizadas, así como ciberdelincuentes y hackers que utilizan la tecnología informática con fines delictivos.

Una de sus actividades es la captura de nombres de usuario y contraseñas. Y una de las formas más efectivas de capturarlas son mediante la técnica del *phishing*.

El delincuente parte de direcciones de e-mail disponibles en sitios web, en redes sociales fácilmente penetrables o en cadenas de spam como solicitudes de apoyo para causas aparentemente nobles.

Esas direcciones "cosechadas" son el blanco de su actividad.

En el *phishing* el delincuente envía a las direcciones de e-mail un mensaje que aparentemente procede de una fuente confiable, como podría ser el administrador del sistema, una dependencia gubernamental o un banco, solicitando códigos de usuario, contraseñas y otros datos personales.

En algunos casos se incluye un enlace para que el usuario incauto haga clic y deposite su información. Es común amenazar con el cierre de las cuentas, demandas judiciales en curso, multas en caso de no proporcionar la información y otras cosas de ese estilo.

Una vez que el usuario incauto obedeció el e-mail de *phishing*, el delincuente utiliza los datos obtenidos, muchas veces de forma inmediata.

Uno de los usos más inocentes es el envío de spam utilizando la cuenta del usuario. Este envío provoca que el dominio de origen (por ejemplo, ort.edu.uy en el caso de la universidad) pase a formar parte de listas negras, dejando incomunicado al dominio de origen con muchos proveedores importantes de e-mail.

En casos peores, el delincuente utiliza la cuenta del usuario para otras acciones: leer su e-mail, robar dinero, extraer otra información útil sobre la organización y realizar ataques informáticos que pueden ser muy perjudiciales.

También puede obtener suficiente información como para robar la identidad de un usuario y actuar en su nombre. Eventualmente, puede personificar al funcionario incauto, realizando en su nombre acciones que pueden ser muy dañinas para la organización y también para la reputación personal y profesional del usuario.

Es evidente que ninguna organización seria solicitará este tipo de datos por correo electrónico. Por tanto, en caso de recibirlo, basta con borrar el mensaje de *phishing* sin tomar ninguna otra acción.

Como se explica en este documento, la contraseña es un elemento secreto que no debe ser proporcionado a nadie, ni dentro ni fuera de la institución. Esta política institucional procura proteger a la organización y a sus funcionarios de acciones y consecuencias como las anteriormente descritas.

En caso de dudas, por favor consultar a DSI.

ANEXO 4 – QUIÉN ENVÍA UN MENSAJE

Cómo verificar el correo electrónico que se recibe

Muchas veces recibimos correos electrónicos maliciosos que afectan la seguridad y confiabilidad de este medio de comunicación:

- **Spam**
  Son correos no solicitados, normalmente de publicidad engañosa, y en grandes cantidades, promoviendo Rolex, Viagra, pornografía y otros productos.

- **Virus informáticos**
  Se propagan mediante archivos adjuntos que pueden infectar el equipo de quien los abre, permitiendo acciones fraudulentas o inconvenientes a terceros.

- ***Phishing***
  Son correos fraudulentos que intentan conseguir información personal, también con el objetivo de acciones posteriores.

- **Engaños (*hoax*)**
  Difunden masivamente noticias falsas o rumores.

- **Cadenas de correo electrónico**
  Consisten en reenviar un mensaje a mucha gente. Aunque parece inofensivo, la publicación de listas de direcciones de correo en los envíos contribuye a la propagación a gran escala del spam y de mensajes con virus, *phishing* y *hoax*.

Debemos estar preparados para identificar estos correos, no solo por su contenido, sino por su origen.

Los campos que normalmente observamos (Asunto, De y Fecha) no bastan para la identificación, porque son fácilmente falsificables.

De hecho, estos mensajes maliciosos casi siempre indican una dirección falsa como remitente del correo electrónico.

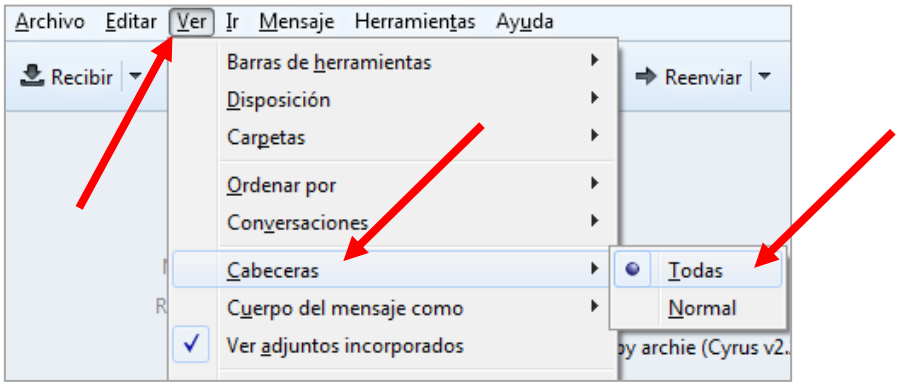
Por esta razón, no se deben responder, ni siquiera para protestar, ya que las respuestas serán recibidas por usuarios que no los enviaron y estaremos propagando el spam, virus o aumentando la confusión general.

Precauciones recomendables

Cuando estemos frente a un mensaje crítico, del cual queremos asegurarnos su origen, una forma es intentar ubicar al remitente por otro medio (por ejemplo, el teléfono).

Es un error suponer siempre que el remitente aparente es el real.

Sin llegar al extremo de llamar por teléfono para confirmar la autoría de un correo electrónico, se puede realizar un primer chequeo estudiando las cabeceras completas de los mensajes (en Mozilla Thunderbird ir a: Ver / Cabeceras / Todas).



En la cabecera completa, los párrafos "Received" indican la ruta que siguió el mensaje, eslabón por eslabón.

Ejemplo:

CASO 1: MENSAJE INTERNO (LEGÍTIMO)

En esta cabecera sencilla hay dos párrafos "Received" y ambos son del servidor archie.ort.edu.uy, ya que el e-mail lo envió rosa@ort.edu.uy desde su correo a (entre otros) hermida@ort.edu.uy, cuyo servidor de correo también es archie.ort.edu.uy.

Y este correo tiene destinatarios visibles (ver párrafo To y CC).

-------- **Mensaje original** --------
Return-Path: <rosa@ort.edu.uy>
Received: from archie.ort.edu.uy ([unix socket]) by archie (Cyrus v2.2.12) with LMTPA; Thu, 22 Oct 2009 17:44:42 -0200
X-Sieve: CMU Sieve 2.2
Received: from [172.30.10.5] (unknown [172.30.10.5]) by archie.ort.edu.uy (Postfix) with ESMTP id E65E11FCED; Thu, 22 Oct 2009 17:44:41 -0200 (UYST)
Message-ID: <4AE0B521.80501@ort.edu.uy>
Date: Thu, 22 Oct 2009 17:40:17 -0200
From: Gabriel Rosa - Coordinador Computacion Distribuida <rosa@ort.edu.uy>
Organization: Universidad ORT Uruguay
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; es-ES; rv:1.9.1b3pre) Gecko/20090223 Thunderbird/3.0b2
MIME-Version: 1.0
To: Coord_labs@ort.edu.uy, Ana Olmedo <olmedo@ort.edu.uy>
CC: Gaston Boero <boero@ort.edu.uy>, Julio Fernandez <Fernandez_J@ort.edu.uy>, Mario Fernandez <Fernandez_M@ort.edu.uy>, Eduardo Hipogrosso <hipogrosso@ort.edu.uy>, Gaston Labadie <labadie@ort.edu.uy>, jaime Damiani <damiani@ort.edu.uy>, Monica Berriolo <berriolo@ort.edu.uy>, Teresa Hermida <hermida@ort.edu.uy>, Daniel Oliveri <oliveri@ort.edu.uy>
Subject: IMPORTANTE : Presupuesto IT 2010.-
X-Priority: 2 (High)
Content-Type: text/plain; charset=ISO-8859-1; format=flowed
Content-Transfer-Encoding: quoted-printable

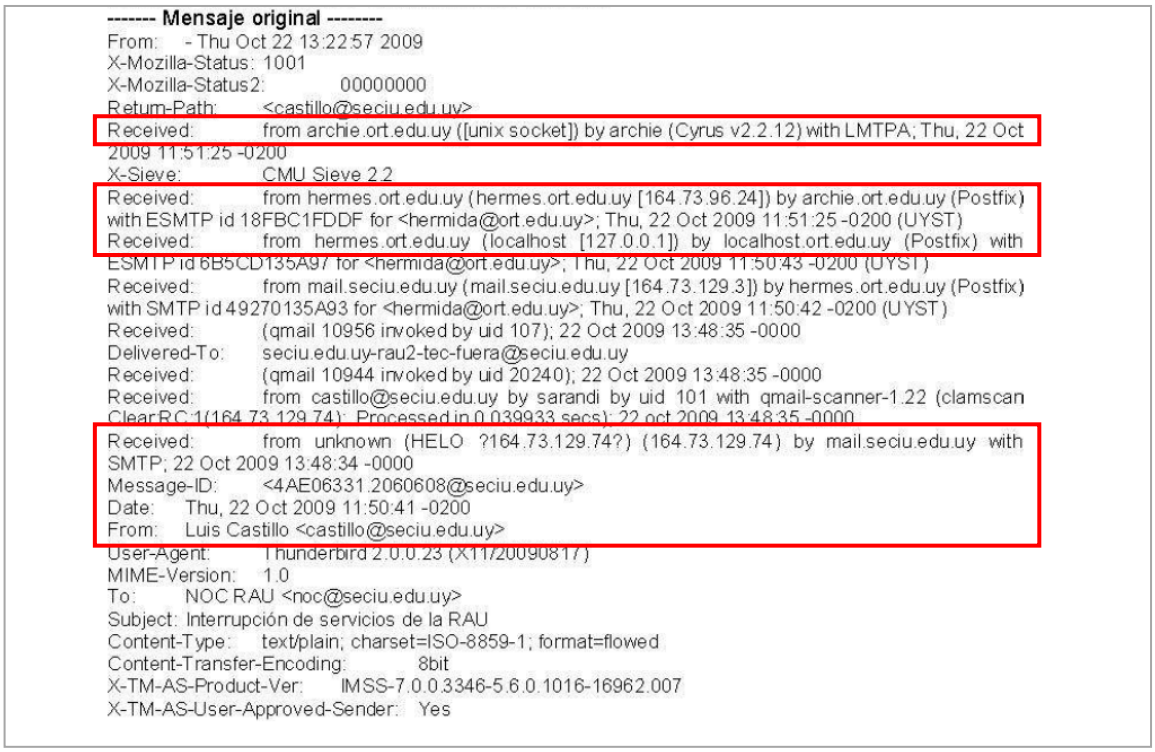
CASO 2: MENSAJE EXTERNO (LEGÍTIMO)

El ejemplo siguiente corresponde a un correo que llegó desde fuera de la universidad.

Siempre el primer párrafo “Received” muestra a nuestro servidor de correo (el último eslabón de la cadena).

En el segundo párrafo “Received” se ve el servidor hermes.ort.edu.uy, que corresponde a nuestro servidor que está al mundo recibiendo los correos externos. Aparece dos veces porque chequea virus.

Y así sucesivamente hasta llegar al último párrafo “Received”, que indica de dónde salió el correo electrónico. Este correo tiene destinatarios ocultos (BCC: o bien CCO:), por lo cual no aparece información al respecto en la cabecera.



------- Mensaje original --------
From: - Thu Oct 22 13:22:57 2009
X-Mozilla-Status: 1001
X-Mozilla-Status2: 00000000
Return-Path: <castillo@seciu.edu.uy>
Received: from archie.ort.edu.uy ([unix socket]) by archie (Cyrus v2.2.12) with LMTPA; Thu, 22 Oct 2009 11:51:25 -0200
X-Sieve: CMU Sieve 2.2
Received: from hermes.ort.edu.uy (hermes.ort.edu.uy [164.73.96.24]) by archie.ort.edu.uy (Postfix) with ESMTP id 18FBC1FDDF for <hermida@ort.edu.uy>; Thu, 22 Oct 2009 11:51:25 -0200 (UYST)
Received: from hermes.ort.edu.uy (localhost [127.0.0.1]) by localhost.ort.edu.uy (Postfix) with ESMTP id 6B5CD135A97 for <hermida@ort.edu.uy>; Thu, 22 Oct 2009 11:50:43 -0200 (UYST)
Received: from mail.seciu.edu.uy (mail.seciu.edu.uy [164.73.129.3]) by hermes.ort.edu.uy (Postfix) with SMTP id 49270135A93 for <hermida@ort.edu.uy>; Thu, 22 Oct 2009 11:50:42 -0200 (UYST)
Received: (qmail 10956 invoked by uid 107); 22 Oct 2009 13:48:35 -0000
Delivered-To: seciu.edu.uy-rau2-tec-fuera@seciu.edu.uy
Received: (qmail 10944 invoked by uid 20240); 22 Oct 2009 13:48:35 -0000
Received: from castillo@seciu.edu.uy by sarandi by uid 101 with qmail-scanner-1.22 (clamscan Clear:RC:1(164.73.129.74): Processed in 0.039933 secs); 22 oct 2009 13:48:35 -0000
Received: from unknown (HELO ?164.73.129.74?) (164.73.129.74) by mail.seciu.edu.uy with SMTP; 22 Oct 2009 13:48:34 -0000
Message-ID: <4AE06331.2060608@seciu.edu.uy>
Date: Thu, 22 Oct 2009 11:50:41 -0200
From: Luis Castillo <castillo@seciu.edu.uy>
User-Agent: Thunderbird 2.0.0.23 (X11/20090817)
MIME-Version: 1.0
To: NOC RAU <noc@seciu.edu.uy>
Subject: Interrupción de servicios de la RAU
Content-Type: text/plain; charset=ISO-8859-1; format=flowed
Content-Transfer-Encoding: 8bit
X-TM-AS-Product-Ver: IMSS-7.0.0.3346-5.6.0.1016-16962.007
X-TM-AS-User-Approved-Sender: Yes

Con los datos de las cabeceras (nombres de servidores y direcciones IP) es posible averiguar qué ruta siguió un correo y si la dirección de origen es verdadera o falsa.

No se pretende que los funcionarios de la universidad analicen toda esta información, pero sí que reenvíen el correo a DSI con las cabeceras completas para analizarlas y determinar su autenticidad, en caso de existir dudas al respecto.

Es importante consultar a DSI si se presenta una situación como las descritas.

ANEXO 5 – MÓDEMS 3G USB

Cuando una computadora que está conectada a la red de la Universidad ORT Uruguay sale a Internet por un canal independiente al previsto en dicha red, como es el caso de los módems 3G, se saltean los elementos de control y protección (como el software antivirus central).

Por tanto, al utilizar módems 3G USB se puede estar habilitando la ocurrencia de ataques de malware que afectarían no solamente al propio equipo del usuario, sino también al resto de la red interna de la universidad, tanto administrativa como académica.

En resumen, el módem 3G USB introduce una conexión directa a Internet que no puede ser protegida ni monitoreada por el software central de la institución y arriesga la seguridad de todos los equipos de la red de la universidad, debido a que el equipo en cuestión puede ser utilizado como una puerta de ataque.

Teniendo en cuenta estos peligros, se debe tener en cuenta lo siguiente:

Está prohibido el uso de módems 3G USB en equipos de la Universidad ORT Uruguay que estén conectados a la red administrativa y/o académica.