DEFENSA DIGITAL PARA ORGANIZACIONES SOCIALES

Mayo - 2021

DEFENSA DIGITAL PARA ORGANIZACIONES SOCIALES

Escrita por: Anais Córdova Páez, Edison Ibañez, Jonathan Finlay;
Editada por: Tatiana Avendaño;
Diseño por: Angie Vannesita

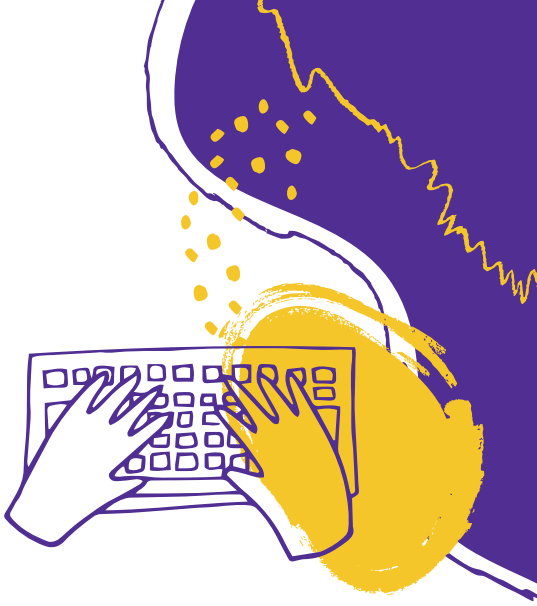
Con el apoyo de:

LaLibre.net

@ DERECHOS DIGITALES América Latina

FONDO DE RESPUESTA + RÁPIDA para la protección de derechos digitales en América Latina

ÍNDICE



INTRODUCCIÓN

El levantamiento social vivido en octubre de 2019 en Ecuador dejó en evidencia algunas de las necesidades más urgentes para el fortalecimiento de las organizaciones sociales, entre las que se encuentra la atención de la seguridad digital. Se trata de la preocupación por la mejora de las comunicaciones y de la seguridad, por el almacenamiento de información y, en general, por los usos de las Tecnologías de la Información y la Telecomunicación al interior de las organizaciones. Cómo una manera de responder al ejercicio del control y la vigilancia por parte del Estado y de instituciones privadas, interesados en bloquear las luchas populares por la defensa de los Derechos Humanos y de la Naturaleza, y también ante los ataques y la censura contra movimientos sociales y personas públicas.

Esta guía es un esfuerzo por sistematizar las experiencias de acompañamiento desarrolladas desde el levantamiento, atendiendo las preocupaciones comunes entre las organizaciones y sus miembros a propósito de la seguridad digital. Partiendo de las urgencias en esta área, a las que no se les ha prestado la suficiente atención entre las demandas de la cotidianidad y las diferentes coyunturas, se proponen seis temas fundamentales para iniciar la defensa digital entre las organizaciones defensoras de Derechos Humanos y de la Naturaleza en Ecuador.

La defensa digital tiene como principio el desarrollo de capacidades para disminuir los riesgos y amenazas en el uso de las tecnologías, desde una visión en la que la autonomía y protección le permita a las organizaciones prepararse para sobrellevar distintos escenarios, con el propósito de fortalecer los procesos internos de la organización y aportar en la continuidad de su trabajo.

Esta guía propone aumentar las capacidades de la organización, desarrollar conocimientos y generar diálogos acerca de las vulnerabilidades, amenazas y riesgos que tienen y viven las organizaciones y sus participantes, remarcando que la seguridad colectiva se sostiene en la seguridad individual de cada de una de las personas que conforman la colectividad.

Este documento plantea de manera sencilla seis temas:

Gestión de riesgos e incidentes digitales: Este tema hace referencia al análisis de riesgos, amenazas e incidentes que comúnmente enfrentan las organizaciones sociales y las personas defensoras de Derechos Humanos, de manera que se dan herramientas claras para leer los peligros y poder reaccionar a ellos.

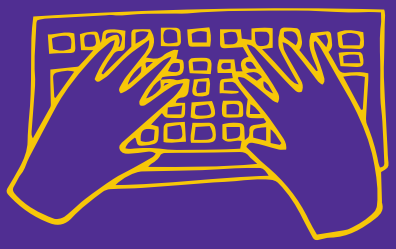
Cifrado: Se da una introducción al tema de la encriptación, explicando su significado y mostrando usos posibles a partir de ejemplos fácilmente comprensibles.

Comunicaciones y correo electrónico seguro: Ante la situación actual, el uso de diferentes medios digitales de comunicación se ha incrementado. En este punto se caracterizan las ofertas de servicios de mensajería instantánea, videoconferencia y correo electrónico, desde la perspectiva de la seguridad y las vulnerabilidades de cada uno, más allá de lo que publicitan sus desarrolladores.

Respaldos: Como hoy en día los equipos electrónicos (laptops, computadoras de escritorio, smartphones, tablets, etc.) contienen toda la información de una persona (laboral y personal), en este capítulo se revisa la importancia de los respaldos periódicos de datos.

Malware y actualizaciones: Este tema desarrolla una introducción sobre el problema del malware, sus diferentes tipos y las estrategias a seguir para mantener la información protegida de posibles ataques.

Plan de Seguridad Digital: Al final de este documento, como anexo, se presenta un borrador que incluye el marco legal para contar con un punto de partida en el planteamiento de un Plan de Seguridad Digital, que permita avanzar en la ejecución de una estrategia de mitigación y reducción de vulneraciones, riesgos y amenazas digitales.



TEMA 1:
INTRODUCCIÓN
A LA DEFENSA DIGITAL

INTRODUCCIÓN A LA DEFENSA DIGITAL

Presentación

La protección de las organizaciones y movimientos sociales depende de la capacidad de afrontar y actuar ante posibles incidentes de seguridad, así como también de su disposición para generar estrategias de defensa y mantenimiento de herramientas activas de protección. Por este motivo, saber identificar los incidentes de seguridad a partir de la comprensión de los riesgos y las amenazas es fundamental para actuar a tiempo en la protección digital y física de las organizaciones de defensores de DDHH.

Es necesario entender que estos riesgos y amenazas dependen de los contextos en donde se desenvuelve la organización, el momento político y la actitud de sus integrantes. Los riesgos y amenazas son siempre cambiantes, por ello, reconocer los incidentes de seguridad permite generar respuestas acordes a cada contexto y a las necesidades de la organización.

Incidentes de seguridad

Un incidente de seguridad es cualquier hecho o acontecimiento que pueda afectar la seguridad personal o de la organización, generando un impacto directo sobre el alcance de su trabajo y posibles acciones en contra de las personas o de toda la organización.

Los incidentes de seguridad no son una amenaza en sí mismos. Sin embargo, requieren que se les preste atención, que sean registrados y que se los analice para poder reaccionar ante los mismos.

El reconocimiento de los incidentes permite cambiar comportamientos o actividades (usos y hábitos para con las tecnologías) con el fin de hacer sostenible el trabajo de la organización, para hacer más seguro su desempeño. Es decir, los incidentes son indicadores de la situación concreta de seguridad en la que se encuentra la organización y sus integrantes. Por ejemplo, después de identificar varios incidentes de seguridad, una organización puede darse cuenta de que la están vigilando: en ese momento puede hacer algo al respecto. Dichos incidentes son indicativos de la magnitud de la oposición al trabajo de la organización o de la presión que soporta la misma.

Todas las personas que trabajan en la defensa de los Derechos Humanos pueden vivir incidentes de seguridad, dado que el impacto de su trabajo genera incomodidad a las grandes corporaciones, a Estados e instituciones. Es importante entender que estos agresores potenciales probablemente ya tengan información sobre los movimientos y actividades de la organización y sus participantes. Entonces la mejor respuesta son las estrategias de protección y mitigación que se puedan construir ante las agresiones en potencia.

Todas las amenazas son incidentes de seguridad, pero no todos los incidentes de seguridad son amenazas.

Protection International, 2020.

¿Por qué suceden las amenazas?

Las amenazas y los riesgos que puede vivir una organización y sus miembros significan que el trabajo que hacen es necesario, y puede haber personas o instituciones que quieran dificultarlo o detenerlo. Para que sea sostenible en el tiempo, es necesario proteger a todos aquellos que trabajan con Derechos Humanos y Derechos de la Naturaleza sin poner en riesgo la vida de las personas que integran las organizaciones, recordando que las acciones personales tienen un impacto colectivo.

Amenazas

Una amenaza es la posibilidad de que alguien tenga intención y pueda dañar la integridad física o moral de otra persona. Una amenaza declarada es una indicación de amedrentamiento para que la persona deje de hacer lo que está haciendo. Toda amenaza tiene las siguientes características: un objetivo, un origen y un medio de expresión, es decir, una manera en que se manifiesta.

Una amenaza es una experiencia individual que tiene un impacto doble: emocional y colectivo. No es lo mismo *amenazar* que constituir una amenaza real, es decir, *ejecutarla*. Muchas veces, no se hacen efectivas, por lo que es posible diferenciar entre amenazas directas e indirectas. Las amenazas, sin embargo, pueden estar cargadas de elementos simbólicos que también afectan el trabajo de las personas.

Las amenazas se asocian directamente con los riesgos, es decir, con las consecuencias potenciales a las que una persona puede enfrentarse si la misma se lleva a cabo.

Existen cuatro puntos para analizar una amenaza que permiten determinar los hechos relacionados con ella: el patrón de cómo se da, el objetivo, el origen y la conclusión razonable sobre dichas amenazas.

Riesgos

Los riesgos son las vulnerabilidades de una organización o persona en función de las amenazas que experimenta, donde se hace referencia a un posible acontecimiento que causa daño. Es importante notar que los riesgos a los cuales está expuesta una organización o persona se encuentran directamente relacionados con las capacidades de mitigación que desarrollan.

El nivel de riesgo al que se enfrenta un grupo de personas defensoras de Derechos Humanos es mayor en relación a las amenazas recibidas, la vulnerabilidad y la capacidad de reaccionar ante ellas. La organización Protection International representa este análisis en una pedagógica ecuación:

$$\text{RIESGO} = \frac{\text{Amenaza x Vulnerabilidad}}{\text{Capacidad}}$$

Dentro de un análisis de riesgo es fundamental como organización o persona entender las amenazas que se enfrentan, reconocer las propias vulnerabilidades e incrementar las capacidades, en función de que exista el menor riesgo posible.

Defensa Digital: casos de análisis de riesgos

El ejercicio de hacer un análisis de riesgos permite a las organizaciones darse el tiempo de incrementar su seguridad y comunicación, y entender sus vulnerabilidades y capacidades. Las organizaciones que trabajan en Derechos Humanos y de la Naturaleza están bajo constante amenaza y riesgo, de manera que realizar este ejercicio les puede permitir mitigar vulneraciones a sus derechos.

Es necesario tomar en cuenta que los riesgos y las amenazas cambian con el tiempo, de acuerdo a cómo va cambiando el contexto, las vulnerabilidades y las capacidades de una organización o persona.

Por lo tanto, realizar un análisis de riesgos periódicamente puede ser fundamental para organizaciones que trabajan en contextos complejos o van a realizar una acción que los puede poner en peligro. Por ejemplo: una demanda al Estado por incumplimiento de la Constitución o una demanda a una empresa petrolera por contaminación.

Aumentar las capacidades en defensa digital toma tiempo, dado que es un trabajo que depende del compromiso de la organización y sus integrantes, que además implica un hábito que se genera a partir de la práctica y que debe ser permanente, porque la actualización constante es fundamental para disminuir las vulnerabilidades.

En caso de que una organización esté bajo ataque, es importante que pueda buscar apoyo de personas de confianza y abrir un diálogo sobre su situación con el fin de conformar un equipo que maneje la misma información.

Para poder realizar un análisis de riesgos se debe tomar en cuenta:

1. Lectura y análisis del contexto.
2. Evaluación del nivel de riesgo al que se enfrenta la organización.
3. Desglose de riesgos: analizar uno por uno para entender y medir su/s impacto/s.
4. Otras cuestiones: ¿Qué hace posible cada riesgo? ¿Qué se debe cambiar en la organización para mitigarlo/s? ¿De acuerdo a los componentes del riesgo, cuáles serían los procesos más coherentes para su mitigación?

Estos cuatro pasos pueden generar claridad sobre cómo proceder en un corto o largo plazo, qué acciones tomar con respecto a la seguridad física, digital y emocional, y en cuanto a medidas legales y de infraestructura.

Bitácora de incidentes digitales

La bitácora es una herramienta del registro marino que permite entender los sucesos y sus cambios en pequeña y gran escala cuando se navega en alta mar, donde las condiciones cambian constantemente. De manera que la bitácora de incidentes digitales tiene el mismo objetivo: registrar eventos, incidentes extraños, amenazas y situaciones de riesgo que afectan a la organización y por lo tanto a sus integrantes, de manera que se pueda hacer un análisis de riesgo.

La bitácora guarda estos incidentes para el análisis en una perspectiva amplia donde es fácil identificar patrones de vulneraciones como llamadas extrañas, censura de la comunicación, persecución a un integrante de la organización, robo y/o pérdida de equipos o documentos, etc. Esta herramienta permite entender dichas vulneraciones para actuar a partir de capacidades y medidas de seguridad.

Es ideal que la bitácora sea responsabilidad de un grupo de personas de la organización a quienes se les reporten los incidentes, y que pueda estar en un lugar seguro para una constante alimentación de registro. En ella se debe registrar la fecha, la hora, el medio y el evento, de manera que se puedan entender los patrones de comportamiento en las agresiones y las vulnerabilidades de la organización y las personas que la conforman.

Fuentes:

- Eguren, E. Caraj, M. 2009. Protección para los Defensores de Derechos Humanos. Protection International. Bélgica . Primera Edición.
- Formación en Línea. Protection International. 2020.
- Enlace web: https://e-learning.protectioninternational.org/?lang=es.

Contraseñas

Al salir de la casa o de la oficina, es posible que se asegure una puerta para que no pueda vulnerarse e impedir la entrada a personas no invitadas. Para lograr esta seguridad se usan llaves que permiten abrir y cerrar, algo que es muy común en el plano físico. De igual manera, en el ámbito digital las claves o contraseñas permiten el ingreso a cuentas personales, espacios habitados en el mundo digital donde se maneja información privada y que no es deseable difundir abiertamente. Por este motivo, las contraseñas juegan un rol fundamental en mantener segura la información. Dedicar tiempo a crearlas y cambiarlas periódicamente es una de las formas más básicas de cuidar la información personal y la de la organización.

Siguiendo esta reflexión, resulta pertinente hacerse estas preguntas: ¿Cuándo fue la última vez que modifiqué mi contraseña de correo electrónico? ¿Lo hago con regularidad? ¿Existe información que deseo proteger en mis cuentas?

En este sitio web es posible probar la fortaleza de una contraseña para entender que tan compleja debería ser: https://howsecureismypassword.net. Esta herramienta calcula el promedio de tiempo en el que una persona o máquina puede descifrar una contraseña.

Una contraseña segura debe tener mínimo doce caracteres, mayúsculas, minúsculas, números y símbolos (· $ % $ & /), puede estar en dos idiomas o ser una canción, poema, libro que te gusta, pero sobre todo debe ser única y específica para cada cuenta en particular. Es importante notar que las contraseñas más seguras son las que recuerdas, aunque es mejor evitar utilizar información relacionada directamente a ti y que es pública como: nombres de un familiar (hijo/a, padre, madre), mascotas o de la organización donde trabajas, fechas de nacimiento.

Cambiar las contraseñas con regularidad es una barrera importante de seguridad simple de lograr

y muy efectiva. Para guardar las contraseñas no es necesario recordarlas todas, lo más práctico y seguro es manejar un administrador de contraseñas. Anotarlas por fuera de un administrador de contraseñas nunca es recomendable, porque siempre puede ser un factor de riesgo.

Administradores de contraseñas

Existen programas que ayudan a administrar contraseñas, es decir, son bases de datos donde se pueden almacenar de manera segura todas las contraseñas y cambiarlas periódicamente. Para ingresar solo se necesita una contraseña maestra, que es como una llave maestra: es decir, basta con recordar una sola contraseña para ingresar a todas las demás. Estos programas pueden ser individuales o colaborativos, aquí se dan algunos ejemplos:

- **Keepass:** Es sumamente popular, puede descargarse en todos los sistemas operativos o en dispositivos celulares.
  https://keepass.info/
- **Psono:** Permite tener contraseñas personales y colaborativas.
  https://psono.com/

PRÁCTICA

A partir de un ejemplo real o ficticio de incidentes, amenazas y riesgos que haya vivido una organización social, realizar un análisis de riesgos para la misma:

1. Describir a la organización (área de trabajo, equipo y relaciones).
2. Explicar el contexto político, económico, social y cultural de la organización.
3. Describir el caso detallando incidentes, amenazas, riesgos, vulnerabilidades y capacidades.
4. Aplicar la fórmula de análisis de riesgo:

$$\text{RIESGO} = \frac{\text{Amenaza x Vulnerabilidad}}{\text{Capacidad}}$$

5. Enumerar los riesgos encontrados.
6. Realizar una bitácora de incidentes de seguridad de este ejemplo, donde se describan cinco incidentes registrados durante un mes. Para poder analizarlos, detallar fecha, medio, descripción, a quién le pasó y quién lo reportó.
7. Instalar Keepass.
8. Crear tu base de datos en Keepass y empezar a administrar tus contraseñas de manera segura.

TEMA 2: CIFRADO

CIFRADO

Introducción

Este capítulo es muy importante, ya que el cifrado es uno de los métodos más efectivos para la protección de derechos en el mundo digital, principalmente el de la privacidad. Permite asegurar que los archivos, mensajes o demás datos almacenados y procesados en los dispositivos personales y de trabajo estén disponibles solamente para el propietario y para las personas a las que éste decide darles acceso.

Cifrar y encriptar son términos que se usan frecuentemente y en distintos ámbitos, pero: ¿Qué es encriptar? ¿Para qué sirve? Y también: ¿cómo se hace?

Según Wikipedia: "En criptografía, el cifrado es un procedimiento que utiliza un algoritmo de cifrado con cierta clave (clave de cifrado) para transformar un mensaje, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave secreta (clave de descifrado) del algoritmo".

Un caso hipotético

Una mañana llegas a tu lugar de trabajo y descubres que las computadoras y demás dispositivos electrónicos han desaparecido. Imagina que en ese momento tú o la organización en la que participas estaba realizando una investigación sobre violaciones a Derechos Humanos. ¿Qué es lo que harías? Supongamos también que en esos equipos tenías testimonios, evidencias, nombres, direcciones y contactos de las personas que sustentan la

denuncia y que, por obvias razones, esa información no debía ser revelada y además imagina que en la investigación han aparecido nombres de varios políticos y funcionarios del gobierno.

En el mejor de los escenarios, quienes se llevaron los equipos los venden por partes o completos, son formateados y toda la información borrada. En el peor de los casos, esos equipos podrían estar siendo analizados y la información que era confidencial podría ser compartida y difundida entre los implicados. Este escenario puede sonar familiar, ya que en muchos países son comunes situaciones como esta. Pero además todo se agudiza cuando una filtración de fuentes puede significar el aumento de la vulnerabilidad de la organización y las personas que la integran, siendo objeto de amenazas, difamaciones, demandas y hasta desapariciones forzadas.

Ahora bien, si en el hipotético escenario se ha incorporado el cifrado de la información, la situación se torna algo menos grave, pues si las claves de descifrado no fueron comprometidas dará igual si los equipos fueron robados para ser vendidos o para buscar en ellos información clasificada, pues de todas maneras la información no será accesible para esos terceros, por lo menos no tan fácilmente.

Glosario

A continuación se listan las definiciones de algunos conceptos para garantizar un entendimiento común que permita el desarrollo del código análogo:

Mensaje: Es lo que se quiere transmitir. Para este ejemplo de cifrado se usarán nombres.

Algoritmo[1]: Es un conjunto de reglas definidas, ordenadas y finitas que permite solucionar un problema, realizar un cómputo, procesar datos o llevar a cabo una tarea. En este caso se usará ROT132[2] como algoritmo de cifrado.

Llaves: En el cifrado existen normalmente dos llaves: una pública (es la que se entrega a quienes

1 https://es.wikipedia.org/wiki/Algoritmo

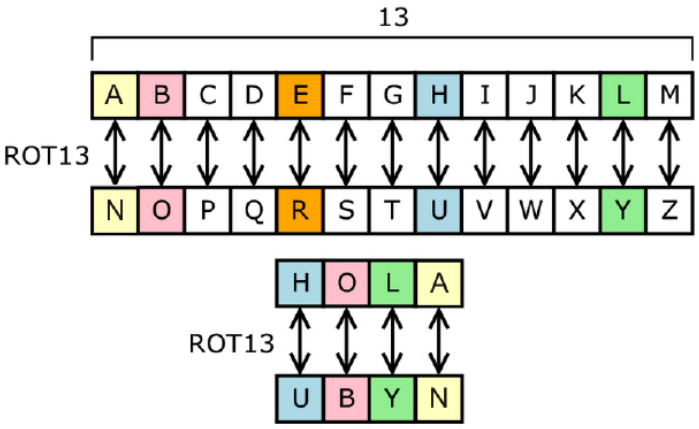
2 https://es.wikipedia.org/wiki/ROT13

van a poder leer los mensajes y que se recibe de las personas que envían mensajes cifrados) y la privada (es la que se usa para cifrar los mensajes y que junto con la llave pública de otra persona permite leer los mensajes que se reciben). Las llaves públicas se comparten y las privadas son confidenciales. Para este ejercicio el algoritmo ROT13 será ambas llaves.

Cifrado: Es el proceso de transformar un mensaje legible por cualquiera a uno nuevo que solo lo pueden leer las personas a las que se les da permiso, o tienen la llave pública de la persona emisora del mensaje.

Descifrado: Es el proceso inverso al cifrado. Significa transformar un mensaje cifrado (ilegible) en uno legible.

Para entender el proceso, se cifra un mensaje utilizando el ROT13, un método que propone hacer un intercambio de letras por sus opuestas conforme a la siguiente ilustración:



La ilustración ejemplifica cómo se puede usar el sistema ROT13 para transformar el mensaje "HOLA" en "UBYN", y el proceso es realmente simple: se reemplaza la H por su opuesta U, la O por B, la L por Y y la A por N.

PRÁCTICA

Para la siguiente práctica primero realizaremos el siguiente ejemplo para decifrar un código.

Ahora, se aplica el algoritmo para transformar el siguiente nombre:

JUANA VEGA.

Entonces, con la ilustración como referencia, las letras correspondientes al mensaje son reemplazadas por su opuesta correspondiente: la J por la W, la U por la H, la A por la N, la N por la A, la A por la N, el espacio queda tal cual, la V por la I, la E por la R, la G por la T y finalmente la A por la N:

ORIGINAL	J	U	A	N	A		V	E	G	A
CIFRADO CON ROT 13	W	H	N	A	N		I	R	T	N

El mensaje cifrado finalmente es:

WHNAN IRTN.

En este caso, el algoritmo es igual a las llaves públicas y privadas antes mencionadas, pues la forma en la que se puede entregar el mensaje "WHNAN IRTN" a otra persona y garantizar su comprensión es indicarle que el procedimiento (algoritmo) que se utilizó para cifrarlo fue ROT13 y que entonces debe usarse el mismo algoritmo para descifrarlo.

Ejercicio: Usando ROT13, descifrar el siguiente mensaje:

UR QRFPVSENQB ZV CEVZRE ZRAFNWR

Cifrar equipos móviles y de escritorio (multiplataforma)

A continuación se mencionan algunas herramientas y recursos que permiten el cifrado de dispositivos. El uso detallado de cada herramienta queda por fuera del alcance de la presente guía, pero se pueden encontrar fácilmente en internet los manuales y recursos necesarios para profundizar en ellos.

Equipos móviles

Android: Google introdujo la funcionalidad "Cifrado de Disco Completo" a finales de 2013 en la versión 4.4 de Android y posteriormente han ido incluyendo mejoras. El proceso es distinto dependiendo de la versión y del fabricante del dispositivo pero para simplificarlo se puede resumir en los siguientes pasos:

- Ir a la configuración del dispositivo.
- Buscar "Seguridad" y luego "Bloqueo de pantalla".
- Seleccionar "PIN", "Patrón" o "Contraseña" (la mejor opción es la de contraseña).
- Activar la opción "Inicio seguro".

iOS: Desde 2014, Apple implementó el cifrado de dispositivos móviles, para activarlo se debe:

- Ir a la configuración del dispositivo.
- Seleccionar "Touch ID & Passcode" (o huella digital).
- Activar "Passcode" (o huella digital).
- Ingresar una contraseña segura

Equipos de escritorio

Veracrypt: Es un software libre multiplataforma. Esto quiere decir que funciona en varios sistemas operativos y es compatible con GNU/Linux, Mac OS y Microsoft Windows. Su característica más desta-

cada es la compatibilidad entre los sistemas antes indicados.

https://www.veracrypt.fr/code/VeraCrypt/

LUKS: Es el sistema de encriptación preferido en los sistemas operativos GNU/Linux. Viene por defecto y es muy fácil de configurar durante la instalación del sistema operativo.

https://github.com/guardianproject/LUKS

FileVault: Es el sistema de cifrado de discos que utiliza Apple en sus sistemas operativos Mac OS. https://support.apple.com/es-co/HT204837

Bitlocker: De los sistemas operativos más utilizados en equipos de escritorio, Microsoft Windows fue el último en ofrecer un sistema integrado para el cifrado de discos. Bitlocker fue introducido recientemente en su sistema operativo Windows 10.

https://support.microsoft.com/es-ec/help/4028713/windows-10-turn-on-device-encryption

Cifrar carpetas

Veracrypt: Además de permitir el cifrado de discos completos (unidades de sistema operativo y externas) también permite crear "volúmenes" cifrados, que son "contenedores" en los que podrás almacenar información sensible sin tener que cifrar todo tu disco.

https://www.veracrypt.fr/code/VeraCrypt/

Cryptomator: Esta es otra interesante opción. Es un sistema de código abierto, que además de funcionar en sistemas de escritorio también es compatible con Android e iOS. Con este sistema al igual que con Veracrypt, podrás crear "contenedores" cifrados de archivos y compartirlos con otras personas o entre dispositivos.

https://cryptomator.org/

PRÁCTICA

1. Crear un volumen o contenedor cifrado con alguna de las herramientas antes mencionadas, cargar algunos archivos y compartirlos con otras personas.

2. Verificar que un dispositivo móvil esté cifrado.

3. Compartir lo aprendido con otras personas de la organización y discutir las ventajas de proteger la información con métodos de cifrado.

TEMA 3:
COMUNICACIONES Y CORREO ELECTRÓNICO SEGURO

COMUNICACIONES Y CORREO ELECTRÓNICO SEGURO

Introducción

En este capítulo revisaremos las comunicaciones y el correo electrónico seguro que, al igual que las contraseñas y el encriptado de archivos, son muy importantes porque hoy en día se han convertido en herramientas indispensables en nuestro día a día, ya sea para conversar con un familiar o para interactuar con compañeros de trabajo.

Por eso es fundamental saber qué tan seguros son los servicios y cómo podemos protegernos y evitar posibles filtraciones de información sensible para nuestra organización.

Mensajería instantánea

Hoy en día las aplicaciones de mensajería instantánea son tan comunes que al momento de comprar un teléfono inteligente ya viene con algunas aplicaciones de este tipo instaladas por defecto (WhatsApp, Messenger, Hangouts, etc.).

La mensajería instantánea es una forma de comunicación entre dos o más personas basado en texto y dispone de ciertas características:

1. Gestión de contactos
    - 1.1. Mostrar distintos “estados”
    - 1.2. Mostrar un mensaje de estado
    - 1.3. Registrar y borrar usuarios de la lista de contactos
    - 1.4. Posibilidad de agrupar los contactos
    - 1.5. Posibilidad de utilizar un avatar

2. Conversación
    2.1. Tipos de mensajes
        2.1.1. Avisos
        2.1.2. Invitación a chatear
        2.1.3. Mensaje emergente
    2.2. Aviso de escritura
    2.3. Uso de emoticones o emojis
    2.4. Charlas en grupo
3. Otras características
    3.1. Envío de archivos
    3.2. Posibilidad de interoperar con otros sistemas de comunicación
    3.3. Utilización de Bots

Como se puede apreciar, estas son algunas de las características que ofrecen los servicios de mensajería instantánea. Pero se conoce como "mensajería instantánea segura" a aquella que se da cuando dos entidades se están comunicando y no quieren a un tercero leyendo o escuchando.

La gran mayoría de los servicios de mensajería instantánea son gratuitos, lo que lleva a cuestionarse cómo mantienen las infraestructuras que los hacen funcionar. Entonces conviene recordar la siguiente frase: "Cuando un producto o servicio es gratuito, tú eres el producto".

Ahora bien: ¿Cómo puede alguien comunicarse de manera segura? Existen aplicaciones que garantizan que la información que se va a compartir a través de ella no se filtrará a terceros. En el siguiente cuadro se puede ver cuáles aplicaciones son seguras:

	Whassap	Messenger	Telegram	Instagram	Hangaouts	Snapchat	Signal
Cifrado	Si	No	No por defecto	No	No	No	Si
Autodestruc-ción	No	No	Si	No	No	¿?	Si
Se guarda en servidores	Si	Si	Si	Si	Si	Si	No
Chats Grupa-les	Si	Si	Si	No	Si	No	Si
¿Quien es el dueño?	Facebook Inc.	Facebook Inc.	Telegram	Facebook Inc	Google, LLC	Snap Inc.	Signal Foun-dation,Sig-nal Messen-ger LLC

Como se puede apreciar, no todas las aplicaciones ofrecen el cifrado de las comunicaciones, por lo que en principio estas aplicaciones no son recomendadas para compartir información o archivos confidenciales. Además, en algunos casos en que ofrecen cifrado lo hacen sin garantizar que las comunicaciones no se filtren, por ejemplo en el caso de WhatsApp, que ha recibido varias acusaciones por filtrado de información de los usuarios.

Videoconferencia segura

Hervé Lambert, jefe de operaciones de la empresa de ciberseguridad Panda Security, afirma: «Por desgracia, no todo el mundo está lo suficientemente concientizado sobre los riesgos que suponen algunas de estas "apps". Por mucho que no queramos usar estas herramientas, en ocasiones no nos quedará más remedio que utilizarlas, porque nuestro jefe o nuestro mejor amigo no quieren aprender a llamar

a través de otra app. Por ello, es importante contar con medidas de seguridad en nuestros dispositivos que eviten que, si nos atacan por medio de alguna de estas apps, sigamos estando protegidos.»[3]

Al igual que los servicios de mensajería instantánea, las aplicaciones o servicios de videoconferencia hoy en día se han vuelto tan comunes que muchas de las actividades colectivas y las reuniones, ya sean de carácter personal o laboral, se hacen a través de algunas de ellas. Sin embargo, éstas no están exentas de problemas de seguridad y pueden potenciar ciertas vulnerabilidades, por ejemplo:

- Poner en riesgo la confidencialidad y la integridad de las comunicaciones.
- Dificultar o impedir la disponibilidad de los participantes en una videoconferencia.
- Obstaculizar el control de acceso, de manera que no se pueda controlar quién accede a una sala o a una reunión privada.
- Facilitar que un tercero suplante a un usuario dentro de una sala o reunión.
- Generar problemas con los permisos del micrófono o la cámara: por ejemplo, permitir que un tercero los controle.

También pueden afectar la videoconferencia generando un mal ambiente o inconformidad entre los asistentes, impedir que se transmita el mensaje o filtrar la información confidencial que se comparte. Además, comprometen la privacidad, ya que muchas veces, al aceptar los "Términos y Condiciones" de uso de estos servicios y aplicaciones, se pasa por alto que se está dando permiso y por lo tanto consentimiento al acceso a información privada y a los archivos (documentos, videos, fotos o imágenes) que se encuentran en los dispositivos de las personas participantes de una reunión.

Si bien no corresponde estigmatizar estos servicios, pues ya sea por temas laborables o personales se necesita hacer uso de los mismos, es importante

3 https://www.abc.es/tecnologia/consultorio/abci-tres-aplicaciones-para-videoconferencias-mas-seguras-202005190152_noticia.html

proteger la información personal o laboral de las personas asistentes a cualquier reunión virtual. Antes de decidir qué servicio utilizar, es necesario hacer una breve evaluación a través de las siguientes preguntas:

- ¿Será usado de forma personal o profesional?
- ¿Se conocen los términos y condiciones de las herramientas a utilizar?
- ¿Se compartirán datos sensibles?
- ¿Participarán personas menores de edad?

Con esta breve evaluación no se podrá evitar totalmente que un servicio sea vulnerado, pero sí se tendrá mayor seguridad al momento de utilizarlo. Lo más importante es ser conscientes del uso que se les da a estas herramientas, y esto se cumple cuando se conoce bien cómo funcionan y, por lo tanto, se puede decidir cómo utilizarlas.

Correos electrónicos seguros

Desde su invención en 1971, el correo electrónico se ha vuelto una parte fundamental dentro de las actividades personales y laborales. Pero, al igual que sucede con todo en internet, no se puede saber quién está del otro lado de un correo electrónico, por lo que hay que tomar ciertas medidas de seguridad para poder verificar el remitente de un correo. Muchas veces se considera suficiente verificar la cuenta de correo del remitente, pero esto no es 100% seguro, ya que no es posible saber si esa cuenta ha sido vulnerada o suplantada. Por lo tanto, la opción más segura es usar una herramienta confiable y especializada para esta tarea.

Esta guía recomienda usar **GNU Privacy Guard o GNUPG**[4], que surgió como reemplazo de **PGP** (Pretty Good Privacy), con la diferencia de que GNUPG es libre y está licenciado bajo **GPL** (General Public Licence).

[4] https://gnupg.org/

¿Cómo funciona? En esta sección se describen tres maneras de utilizarlo. Como se explicó en el capítulo de cifrado, **GNUPG** (o GPG) funciona generando un par de llaves, una pública y otra privada:

- **La clave privada:** como su nombre lo dice, no debe compartirse con nadie. Lo ideal es poder guardar un respaldo de ésta en un lugar seguro.
- **La clave pública:** en oposición a la clave anterior, ésta es la que se puede compartir con los contactos para que puedan verificar nuestra identidad y para que puedan enviarnos correos cifrados. Es conveniente subir esta clave a un Servidor de Claves (por ejemplo, pgp.mit.edu), que es un directorio en el que se puede buscar la clave pública de cualquier contacto para poder enviarle un correo firmado y cifrado. No importa a cuál servidor se suba esta clave, ya que estos comparten información entre sí.

Recursos

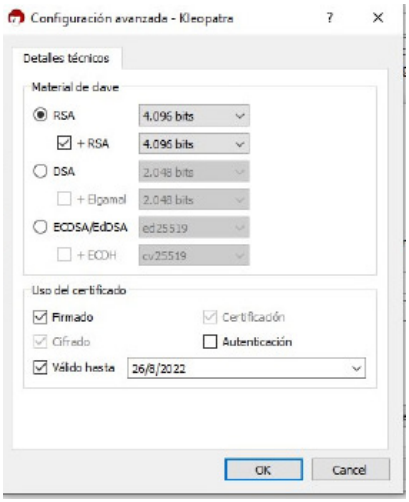
GNUPG: Instalación y configuración inicial

GNUPG es una herramienta de línea de comandos con características ideadas para una fácil integración con otras aplicaciones gráficas. Se instala en el sistema operativo descargando uno de los binarios que se encuentran en el sitio oficial del proyecto (https://gnupg.org). Es una herramienta multiplataforma disponible para para MS Windows, Mac OS y GNU/Linux. Se instala haciendo uso del sistema de gestión de paquetes correspondiente y existen aplicaciones gráficas que simplifican su usabilidad.

Indistintamente de cómo se generen el par de claves GNUPG, es necesario tomar en cuenta los siguientes parámetros al momento de crearlas:

1. **Tipo de cifrado:** al momento de generar una clave el asistente da opciones para escoger el tipo de cifrado. Es importante seleccionar “RSA” y marcar las opciones de “Firmar” y “Cifrar”.

2. **Fortaleza de la clave:** aquí el asistente da la opción de seleccionar un rango entre 1024 y 4096 bits. Es recomendable escoger 4096 bits, ya que esto resultará en una combinación aleatoria de caracteres más robusta.
3. **Fecha de caducidad:** en este apartado se puede escoger el tiempo de vigencia de la clave. Es aconsejable delimitar el tiempo de uso para poder renovar dichas claves de manera periódica.
4. **Información opcional:** Adicional a los puntos antes mencionados, el asistente pide también algunos datos de identificación como nombre/s y apellido/s, correo electrónico y un comentario (esto hace parte de la información que puede ser visible).



(Las imágenes anteriores fueron tomadas usando **Kleopatra** que viene incluido dentro del paquete **Gpg4win**[1],[5] para MS Windows.)

Una vez llenada la información que pide la aplicación para generar el par de claves, también va a pedir una "frase contraseña" que servirá como contraseña maestra para los archivos y correos cifrados con GNUPG. Si no se establece este parámetro, la clave puede ser vulnerable, ya que cualquiera que logre obtener el archivo de la clave privada va a poder

5 https://gpg4win.org/download.html

descifrar los archivos o correos cifrados sin necesidad de utilizar este segundo factor de autenticación.

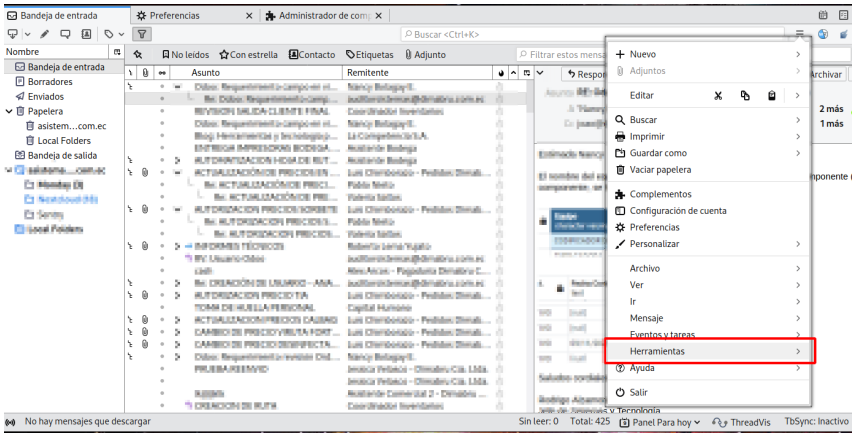
Ya con la clave generada se puede hacer uso de la misma. Si se está trabajando en MS Windows, al momento de instalar Gpg4win también se instalará un complemento para MS Outlook que permite enviar correo cifrado, pero también se podrá usar sin problemas con otro cliente de correo, como Thunderbird.

Usando Thunderbird

Thunderbird desde la versión 78 en adelante, cuenta con un cliente nativo para usar **GNUPG**, ya que incorporaron en su equipo de trabajo al fundador del proyecto Enigmail[6] (Complemento recomendado para usar **GNUPG** con en versiones anteriores de Thunderbird), por lo que no es necesario instalar ningún complemento adicional.

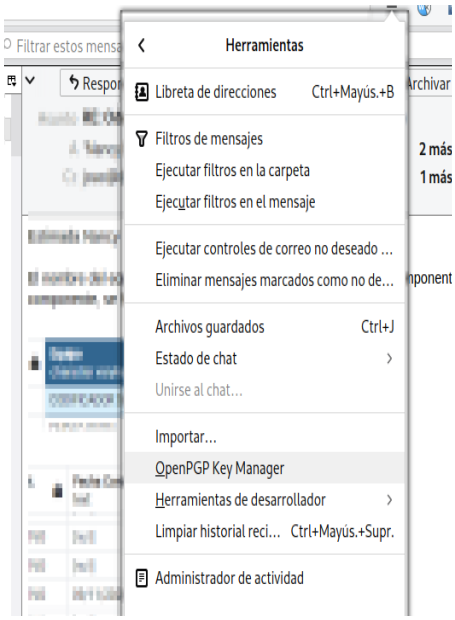
Para empezar a usar el gestor de claver GNUPG en Thunderbird, tenemos que seguir los siguientes pasos:

1. Ingresamos al menú Herramientas.

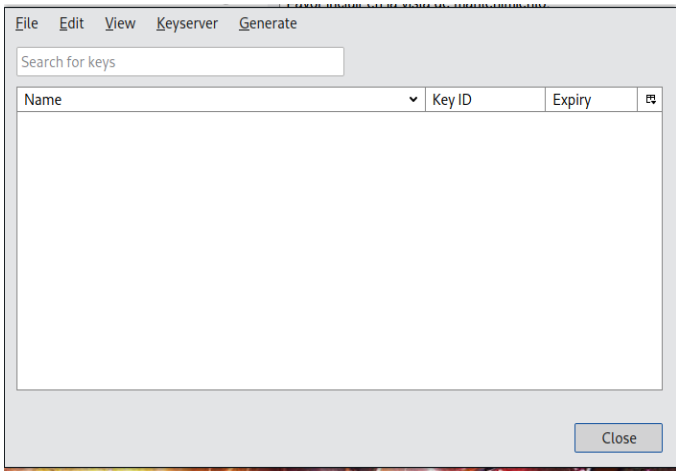


6 https://blog.thunderbird.net/2019/10/thunderbird-enigmail-and-openpgp/

2. Dentro de este menu encontraremos la Opción OpenPGP Key Manager o Gestor de claves OpenPGP:



3. Una vez selecionada esta opción podemos empezar a gestionar nuestras claves **GNUPG**



Siguiendo estos pasos ya se está capacitado para enviar y recibir correos cifrados.

Correos seguros desde el navegador

También es posible enviar correos electrónicos seguros desde el navegador, haciendo uso del complemento **Mailvelope** (https://www.mailvelope.com/en) que permite hacer uso de GNUPG directo desde la web sin necesidad de un cliente de correo.

Si bien estos pasos pueden llegar a ser complicados o confusos, también existen alternativas que ya ofrecen integradas todas las seguridades antes mencionadas en esta sección. Las más populares son:

- **Protonmail:** es un servicio de correo electrónico cifrado, creado en 2013 por los científicos e ingenieros del CERN Jason Stockman, Andy Yen y Wei Sun a raíz de las revelaciones del ex trabajador de la CIA, Edward Snowden, sobre las prácticas de vigilancia masiva de las agencias de seguridad estadounidenses[7].

  https://protonmail.com

- **Tutanota:** es el primer servicio de correo encriptado de extremo a extremo que encripta todo el buzón, en este caso iniciado antes de las filtraciones de Snowden en 2011. Con su tecnología única de código abierto, Tutanota lucha por la privacidad y la libertad de expresión en línea, permitiendo que todos, incluidas las ONG, periodistas y activistas, envíen correos electrónicos cifrados en computadoras de escritorio y dispositivos móviles. Además, la asequible versión comercial de Tutanota permite a las empresas y organizaciones de todos los tamaños proteger fácilmente sus comunicaciones por correo electrónico.[8]

  https://tutanota.com/es/

7 https://es.wikipedia.org/wiki/ProtonMail

8 https://tutanota.com/es/about/

PRÁCTICAS

1. Generar un par de claves GNUPG usando alguno de los métodos antes mencionados.
2. Configurar Outlook, Thunderbird o Mailvelope con la clave que se acaba de generar.
3. Enviar la clave pública a un contacto (cuando se envía la clave pública no se debe enviar cifrado el mensaje, ya que la persona que la reciba no la va a poder importar dentro de su Gestor de Claves).
4. Solicitar la clave pública de un contacto.
5. Enviar un correo cifrado.
6. Analizar los servicios como Protonmail o Tutanota y ver si se ajustan a las necesidades de la organización.

TEMA 4:
Respaldos

RESPALDOS

Realizar respaldos de información

En los dispositivos electrónicos se guarda mucha información (fotos, archivos de estudio, trabajo, claves, etc.) que resulta indispensable en el día a día. ¿Qué pasaría si cuando se trata de acceder a uno de estos documentos no se puede visualizar, ya sea por un fallo del disco, un fallo eléctrico, una infección por la instalación de algún software malicioso o, en el peor de los casos, porque se extravió o fue robado dicho equipo?

La respuesta es simple: se puede recuperar toda la información con un respaldo (siempre y cuando, se haya hecho con anterioridad). Un respaldo hecho oportunamente permite recuperar toda la información y estar nuevamente operativos en cuestión de horas.

En 2017, ESET[9] realizó una encuesta que demostró que el 91% de la comunidad entrevistada en Latinoamérica sí respalda su información. Pero, ¿con qué frecuencia lo hacen?

¿Qué información se debe respaldar?

La información que se debe tomar en cuenta a la hora de hacer un respaldo es aquella que sea más difícil de recuperar o recrear (por ejemplo: fotos, trabajos académicos, proyectos y claves).

¿Qué tipo de respaldo se debe elegir?

Algunas personas optan por sacar un respaldo total del equipo en cuestión, otras los archivos más importantes y otras solo respaldan archivos de configuración del sistema. Esto depende totalmente de la necesidad de cada persona, ya que se debe tomar en cuenta el espacio

9 Fundada en 1992, ESET es una compañía global de soluciones de software de seguridad que provee protección de última generación contra amenazas informáticas: https://somoseset.com/la-compania/

de almacenamiento disponible en donde se vaya a almacenar dicho respaldo (disco duro, CDs, DVDs o incluso en la nube).

¿Qué tipo de almacenamiento se debe elegir?

Como se mencionó anteriormente, se debe contar con espacio suficiente para almacenar el o los respaldos. Si se hace en un disco duro externo es recomendable que el uso de éste sea exclusivo para el almacenamiento de respaldos, para evitar que se deteriore por un uso excesivo. Los medios ópticos no son recomendables por su uso y almacenamiento limitados, entonces esto deja como opción alojarlos en internet. Pero no todos los servicios de almacenamiento en la nube (internet) son recomendados para esta tarea, ya que por ejemplo en el caso de Google Drive éste no garantiza que la información esté segura y que nadie más vaya a tener acceso a ella.

Pero existen opciones como **Mega.nz** (https://mega.nz/), que cifra toda la información que se almacena en ella, o **Nextcloud** (https://nextcloud.com/) que permite levantar una nube propia.

Frecuencia de respaldo

Esto, como se mencionó anteriormente, depende de la necesidad de las personas. Algunos preferirán sacar un respaldo al mes, otros cada semana y otros a diario. Pero si se busca que el tiempo de respuesta ante cualquier daño de un equipo o dispositivo sea rápido, lo ideal es tener un respaldo lo más actualizado posible para así minimizar la pérdida de información.

Recursos

Una vez entendido que es muy importante realizar un respaldo periódico de la información, surgen las siguientes preguntas: ¿Cómo sacar un respaldo? ¿Basta con copiar los archivos de un lugar a otro? ¿Qué programas se pueden utilizar para esta tarea?

Existen varias herramientas para realizar respaldos. A continuación se listan algunas de acuerdo al sistema operativo:

- Guía de DragonJar para GNU/Linux: Herramientas para Backup linux
- Guía de Nettix para MS Windows: Herramientas para Hacer Backup en Windows 10
- Para Mac OS: La mayoría de alternativas que existen para MS Windows también tienen su versión para Mac OS, por lo que no es necesario listar alternativas que funcionen únicamente para este sistema operativo.

PRÁCTICAS

1. Analizar y ordenar la información que es indispensable y que debe estar respaldada.
2. Analizar qué herramienta es más conveniente para hacer un respaldo.
3. Analizar con qué frecuencia conviene hacer un respaldo de la información importante.
4. Buscar un servicio de almacenamiento que se ajuste a las necesidades para almacenar uno o más respaldos.

TEMA 5:
MALWARE Y ACTUALIZACIONES

MALWARE Y ACTUALIZACIONES

Malware

Se puede comenzar respondiendo algunas preguntas básicas: ¿De qué protege un antivirus? ¿Qué es un virus informático? Y finalmente: ¿Existen otras amenazas aparte de los virus? Ya hace muchos años que se escucha hablar de virus y antivirus. Este capítulo tiene el objetivo de explicar qué es lo importante sobre ellos y cómo proteger los dispositivos de potenciales invasiones.

A pesar de que es común hablar de "antivirus", los programas que reciben ese nombre son en realidad antimalware. El antimalware es un software que pretende proteger equipos y dispositivos contra varios tipos de software y programas maliciosos que afectan de distintas maneras los dispositivos. Para entender mejor este tema se listan algunos de los tipos más comunes de malware:

Virus informáticos

Se llaman así debido a que su comportamiento es similar al que tienen los virus en los cuerpos orgánicos, es decir:

- Requieren de un anfitrión para reproducirse.
- Una vez que el anfitrión ha sido infectado, realizan múltiples copias de sí mismos.
- Buscan infectar a otros (por uno o diversos medios).

Los virus buscan:

- Replicarse (crear copias de sí mismos).
- Causar problemas de velocidad en el equipo infectado.
- Saturar los recursos.

Como los virus biológicos que afectan a personas y animales, los virus informáticos destruyen o corrompen el funcionamiento del anfitrión, dejando el sistema sin capacidad de recuperarse. Entonces cuando se habla de antivirus, en informática, se alude a los programas de defensa contra los virus.

Troyanos

El Caballo de Troya[10] se trató de un artilugio en forma de una enorme escultura de madera que permitió a los aqueos engañar a los troyanos. Ofreciéndolo como tributo a su supuesta derrota, los troyanos lo introdujeron dentro de la ciudad amurallada y por la noche de su interior salió un grupo de soldados que, matando a los centinelas, permitieron luego ingresar al ejército aqueo, lo que causó la caída definitiva de Troya.

En informática, se llama "troyano" a cualquier programa que toma la forma de otro ocultándose en su interior espera que un usuario despistado o desinformado lo ejecute. A partir de ese momento puede tomar control completo del equipo y desde entonces permitir a quien lo desarrolló controlar de manera remota la computadora infectada y todos los dispositivos conectados, e incluso realizar acciones como, por ejemplo, encender la cámara sin permiso, leer información de los discos, imprimir documentos o cambiar los parámetros de conexión a internet, entre muchas otras.

Gusanos

También se los conoce por su nombre en inglés: worms. Este tipo de malware busca destruir y saturar equipos, redes e infraestructura. Se replica rápidamente y es altamente dañino. Este tipo de malware ha llegado a bloquear incluso centrales eléctrícas, nucleares y otras grandes infraestructuras de cómputo en todo el mundo. Se puede decir que es un tipo de virus pues comparte varias de sus carac-

10 https://es.wikipedia.org/wiki/Caballo_de_Troya

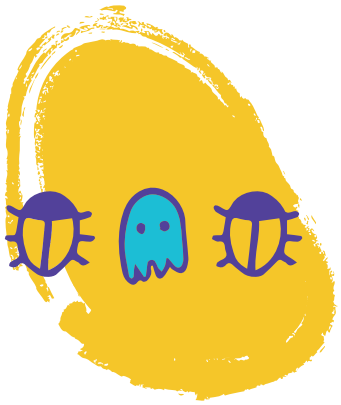
terísticas, aunque la diferencia fundamental consiste en que no infectan archivos en la computadora.

Spyware

Su nombre ya sugiere su propósito y es que este tipo de malware se especializa en espiar. Se trata de un software que lo que pretende es recopilar la mayor cantidad de información de su víctima u objetivo y enviarla a terceros. Existen muchísimos de estos sistemas, inclusive los hay de uso gubernamental y empresarial. Para profundizar un poco más al respecto, se recomienda el artículo "NSO Group suplantó a Facebook para instalar malware de vigilancia" de R3D, Red de Defensa de Derechos Digitales.[11]

Ransomware

Por último, y no porque sea menos importante, hay que mencionar al ransomware. En el último tiempo este tipo de software malicioso se ha popularizado porque han sido miles las personas afectadas por diferentes productos de este tipo. ¿Qué es lo que hace? Su nombre lo sugiere: ransom es una palabra inglesa que significa "rescate". Funciona de la siguiente manera: al infectar un equipo o dispositivo, el malware se activa e inicia un proceso de encriptación de todos los documentos no esenciales para el sistema operativo. Este proceso es transparente, ya que se puede notar algo de lentitud en el funcionamiento de la computadora. Una vez que ha terminado el proceso (lo cual depende de la cantidad de datos), la información y los archivos dejan de ser accesibles y, normalmente, el fondo de escritorio cambia o aparece una ventana como la que se muestra a continuación, con las instrucciones para el "rescate":



11 https://r3d.mx/2020/05/20/nso-group-suplanto-a-facebook-para-instalar-malware-de-vigilancia/

Algunos de los ataques de ransomware han tenido solución pero la mayoría no, esto significa que los archivos de las personas afectadas permanecieron inaccesibles con la pérdida que ello implica.

¿Cómo puede llegar un malware a un equipo?

Los vectores de infección más comunes son dos. El primero es por medio del uso de software "pirata". Esto se debe a que, si bien existen muchas personas que desbloquean (o crackean) los programas de la computadora para permitir a otras su uso y socializar el conocimiento, hay terceros que buscan beneficiarse o causar daño.

El segundo modo más común es por medio de enlaces de internet o archivos, que pueden llegar por medio de correos electrónicos extraños o no deseados, o también por medio del uso de memorias flash u otros dispositivos de almacenamiento.

¿Cómo protegerse contra los malwares?

- Usar un antivirus o antimalware en los equipos.
- Al insertar una memoria flash u otro dispositivo de almacenamiento, permitir al antivirus analizarlo.

- Evitar abrir enlaces en mensajes de texto, correos, chats y descargar archivos adjuntos extraños o de remitentes desconocidos.
- Utilizar siempre páginas web seguras (https).
- Actualizar regularmente sistemas operativos y programas.
- Al instalar un antivirus, puede ser más conveniente una versión gratuita que una versión completa "pirata".
- Mantener el antivirus actualizado (solo se puede tener un antivirus funcionando a la vez en cada equipo, poner más de uno puede hacer que el equipo falle).
- Nunca pero nunca hacer caso a anuncios en páginas web en los que se indica que se han detectado amenazas en un equipo. Todos estos anuncios son un engaño.

Actualizaciones

Se suele pensar que las actualizaciones son molestas e innecesarias. Lastimosamente algunos fabricantes de software como Microsoft han hecho que sean muy molestas, pero siempre (o casi siempre) son necesarias, puesto que lo que hacen es mejorar algunos problemas o errores que han sido detectados en los sistemas y programas. Por ejemplo, una actualización de Windows corrige problemas en el sistema operativo, mientras que una actualización de la base de datos del programa antivirus agrega nuevas capacidades para la detección y eliminación de malware. Sucede lo mismo en el caso de actualizaciones de cualquier otro tipo de aplicaciones en todo tipode dispositivo.

Las actualizaciones son entonces importantes pero, en algunos casos, traen también algunos riesgos:

- En algunos casos, el software advierte sobre la necesidad de hacer un respaldo previo y hacerlo puede evitar muchos problemas más adelante.

- Los programas “piratas” suelen recomendar la desactivación de los antivirus o de las actualizaciones del sistema operativo y esto puede causar otros problemas.

Por lo general, el uso del sistema operativo libre GNU/Linux es por defecto suficiente para cualquier persona que usa su computadora para navegar en internet, comprar y vender productos, usar redes sociales, desarrollar documentos y mantener comunicaciones. Por lo tanto, la mejor recomendación en torno a la seguridad digital es comenzar a investigar las bondades de usar sistemas operativos basados en software libre (https://es.wikipedia.org/wiki/Software_libre). Sistemas operativos como Debian, Linux Mint o Fedora, entre otras opciones, traen por defecto una suite de ofimática y sus actualizaciones son libres y gratuitas, por lo que sin mucho esfuerzo es posible tener toda la información resguardada.

Recursos

Algunos de los antivirus gratuitos con mejor reputación en orden alfabético son los siguientes:

- **AVG:** https://www.avg.com/es-ww/free-antivirus-download
- **Avira:** https://www.avira.com/es/free-antivirus-windows
- **Bitdefender:** https://www.bitdefender.com/solutions/free.html
- **Karsperky:** https://latam.kaspersky.com/free-antivirus
- **Malwarebytes:** https://es.malwarebytes.com/mwb-download

Y algunos recursos sobre actualizaciones:

- Guía GenBeta: Cómo actualizar Windows a la última versión (muestra el paso a paso para Windows 7, 8 y 10)
- Guía de Google: Cómo consultar y actualizar tu versión de Android
- Guía de Apple: Actualizar el iPhone, iPad o iPod touch

PRÁCTICA

1. Instalar uno o varios de los antimalware/antivirus gratuitos en una computadora y en un teléfono celular. En caso de instalar más de uno, desactivar o desinstalar siempre el anterior, ya que solo uno puede quedar activo.

2. Revisar el estado de equipos con respecto a las actualizaciones automáticas.

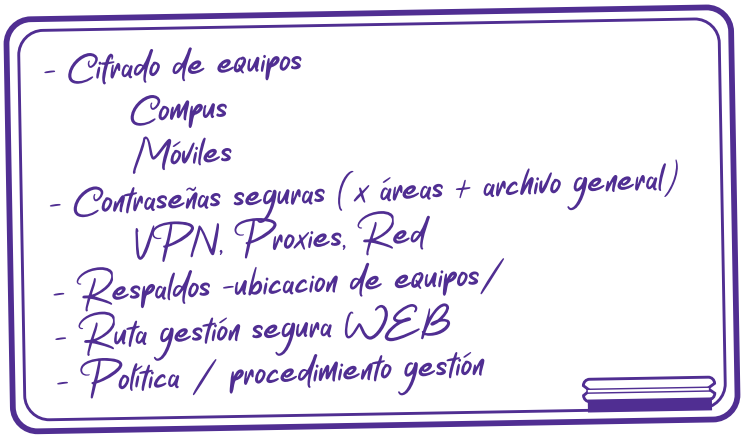
ANEXO:
PLAN DE SEGURIDAD DIGITAL

PRESENTACIÓN

[Las principales preocupaciones que tienen las organizaciones a la hora de pensar en su seguridad digital son el marco legal y el soporte de la documentación. Este documento permite sentar las bases y perfilar una estructura formal para abordar una estrategia integral.]

En julio de 2020 se realizó el curso de Protección Digital para Organizaciones Sociales, que tuvo una duración de 40 horas y fue facilitado por talleristas del proyecto LaLibre.net Tecnologías Comunitarias. Las necesidades y preocupaciones relacionadas con la seguridad digital y tecnologías de la información que surgieron durante el curso son abordadas en el presente plan.

[La mejor forma de iniciar este proceso es con una reunión interna, lo más amplia posible, en la que se piensen los retos y las necesidades que tiene la organización y todas las personas que la componen. Una lluvia de ideas (como muestra la imagen inferior) puede servir como base. Es importante que el proceso se haga hacia adentro de la organización y que todas las personas puedan participar y proponer.]



[Preguntas que pueden guiar la lluvia de ideas: ¿Qué información producimos? ¿Qué información intercambiamos? ¿Manejamos información sensible? ¿Qué medios usamos para trabajar con esta información? ¿A qué riesgos estamos expuestas y expuestos? ¿Qué pensamos que deberíamos hacer mejor a la hora de manejar la información con la que trabajamos?]

El objetivo del presente documento es definir un plan de mejoras en Tecnologías de la Información (TI) para la organización, aplicable en un intervalo razonable de tiempo. En base a lo expuesto anteriormente, se propone un año para la ejecución del Plan, estableciendo objetivos medibles y cuantificables que permitan a la organización y a las personas:

- Desarrollar, aprobar e implementar una Plan de Seguridad Digital basada en el Sistema de Gestión de Seguridad de la Información (ISO 27001).
- Actualizar periódicamente el Plan de Seguridad Digital conforme su avance, las necesidades y recursos de la organización.

PLAN DE SEGURIDAD DIGITAL

ANTECEDENTES (MARCO LEGAL NACIONAL E INTERNACIONAL)

El artículo 12 de la *Declaración Universal de los Derechos Humanos*, adoptada por la Asamblea General de Naciones Unidas, establece que el derecho a la vida privada es un derecho humano:

> » Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

El artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, adoptado por la Asamblea General de Naciones Unidas, consagra al respecto lo siguiente:

> » 1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, o lugar físico, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.
>
> » 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

La *Constitución de la República del Ecuador* en el capítulo sexto, "Derechos a la Libertad", en su art. 66, reconoce y garantiza:

- El derecho al honor y al buen nombre. La ley protegerá la imagen y la voz de la persona.
- El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión

de estos datos o información requerirán la autorización del titular o el mandato de la ley.

- El derecho a la intimidad personal y familiar.
- El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación.

La *Ley Orgánica de Comunicación* en su art. 31, "Derecho a la protección de las comunicaciones personales", expide:

> Todas las personas tienen derecho a la inviolabilidad y al secreto de sus comunicaciones personales, ya sea que éstas se hayan realizado verbalmente, a través de las redes y servicios de telecomunicaciones legalmente autorizadas o estén soportadas en papel o dispositivos de almacenamiento electrónico.

[Si esta cita también es pertinente en el caso de tu organización, puede agregarse al Plan. Si no, puedes quitarla:

El *Reglamento del Sistema de Protección a Testigos y Víctimas*, en su artículo 3, "Principios", informa:

> El Sistema de Protección y Asistencia a Víctimas, Testigos y Otros Participantes en el Proceso Penal se regirá por los siguientes principios: [...] **Reserva y confidencialidad.**- Toda documentación y aspectos relativos al procedimiento de protección se mantendrán bajo estricta reserva, obedeciendo al principio de confidencialidad, obligación que deberá ser cumplida por todas las instituciones involucradas en el Sistema.]

El presente documento establece un marco de referencia para mejorar la seguridad y gestión de los activos de información de **[nombre de tu organización]** y propone la implementación del Sistema de Gestión de Seguridad de la Información según establecido en las Normas Técnicas Ecuatorianas NTE/INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información en lo que sea relevante, pertinente y que brinde valor a la organización.

Declaración

La organización **[nombre de tu organización]** implementará un Sistema de Gestión de Seguridad de la Información cumpliendo con los principios de confidencialidad, integridad y disponibilidad de sus activos de información, promoviendo una gestión de riesgos y una cultura de seguridad.

Descripción

Por medio del presente se busca incorporar en los procesos de gestión interna políticas, normas y procedimientos para la seguridad de la información, así como la aplicación de estándares mínimos en el uso, almacenamiento, acceso y distribución de la información.

Por lo tanto, es absolutamente necesario que todas las personas que participen en la gestión de información de la organización cumplan las normativas que se dicten y estén vigentes, a través de la implantación de un Sistema de Gestión de Seguridad de la Información orientado al resguardo de los activos de información.

El documento, las directrices y los alcances son susceptibles de mejora continua, siendo factibles las modificaciones, actualizaciones y cambios periódicos que la organización considere pertinentes.

Objetivos

- Identificar, clasificar, categorizar y mantener actualizados los activos de información.
- Identificar a las y los responsables de la seguridad de los activos de información.
- Determinar los roles, responsabilidades y competencias de las y los miembros de la organización que tengan relación con los activos de información.
- Proteger, resguardar y asegurar la disponibilidad, integridad y confidencialidad de los activos de información y tecnologías para su procesamiento.
- Detectar, eliminar o mitigar las vulnerabilidades y los riesgos que amenacen los activos de información.
- Establecer, actualizar y difundir normas, procedimientos e instructivos para la manipulación, uso y resguardo adecuado de los activos de información.
- Monitorear y mantener actualizado el Sistema de Gestión de Seguridad de la Información, y establecer los mecanismos de seguimiento y control de los activos de información y tecnologías de procesamiento.
- Difundir el Plan de Seguridad Digital y capacitar a todas las personas que trabajan con la organización.

Roles y responsabilidades

Para dar seguimiento, continuidad y cumplimiento a lo establecido en la Plan de Seguridad Digital, se establecen los siguientes roles y responsabilidades:

[Definir desde la organización, qué persona o grupo de personas asume los siguientes roles]

Oficial de Seguridad digital

Persona que cumple la función de supervisar el cumplimiento del presente plan y de coordinar las funciones del comité. Su función es liderar el establecimiento, la implementación y el mantenimiento del Sistema de Gestión de Seguridad Digital.

Comité o Asamblea de Seguridad de la Información

Es un cuerpo integrado por personas de la organización, destinado a asegurar la implementación del Sistema de Gestión de Seguridad Digital. Sus funciones son: proponer, impulsar, promover y revisar periódicamente el Sistema de Gestión de Seguridad Digital.

Responsable de TI

Persona que cumple la función de cubrir los requerimientos de seguridad informática establecidos y supervisar las tareas de implementación y mantenimiento de sistemas.

Miembros de la organización

Personas que usan los activos de la información y los sistemas para su procesamiento. Son las y los responsables de conocer, cumplir y hacer cumplir el plan y los procedimientos de seguridad digital. Tienen, además, la responsabilidad de reportar incidentes de seguridad.

Glosario

Sistema de Gestión de Seguridad de la Información (SGSI)

Es un conjunto de procesos que permiten gestionar la seguridad de la información de forma sistemática. Estos procesos serán levantados sobre la base de un enfoque de mejora continua. Un SGSI parte de una evaluación de riesgos en la que se definen medidas de mitigación de aquellos riesgos que se evalúen como inaceptables y contempla una mejora continua con el objetivo de que madure el sistema a lo largo del tiempo.

Activos de Información

Comprende a los sistemas de información, aplicaciones o herramientas de tipo software, bases de datos, equipos computacionales, dispositivos móviles, archivos físicos, documentos electrónicos o cualquier otro activo que por su naturaleza registre, procese, almacene o transmita información.

La información es uno de los activos más importantes de las instituciones y organizaciones, en todas las formas en que ésta se manifieste: textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales; y en todos los medios de almacenamiento: magnéticos, ópticos, electrónicos o impresos.

Seguridad de los Activos de Información

Se trata de proteger, resguardar y asegurar la disponibilidad, confidencialidad e integridad de los activos de información y tecnologías implicadas para su procesamiento, a efecto de garantizar la continuidad operacional de la organización.

Matriz de riesgos

Documento que permite mapear los principales riesgos y amenazas a la seguridad de la información

de una organización. También permite describirlos y analizar el estado de cada uno, además de dar pie a un plan para su mitigación.

Confidencialidad

Se garantiza que la información sea accesible solamente a aquellas personas autorizadas a tener acceso a la misma. (SNAP, 2013)

Disponibilidad

Se garantiza que las y los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella, toda vez que lo requieran. (SNAP, 2013)

Integridad

Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento. (SNAP, 2013)

Referencias

1. Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27000, es una traducción idéntica de la Norma Internacional ISO/IEC 27000:2016, Information technology — Security techniques — Information security management systems — Overview and vocabulary. El Servicio Ecuatoriano de Normalización, INEN, es el responsable de la traducción de esta Norma Técnica Ecuatoriana.
2. Esquema de Seguridad de la Información EGSI. Registro Oficial Suplemento No. 88 del 25 de septiembre del 2013.
3. Política de Seguridad de Información en el Ministerio de Telecomunicaciones y de la Sociedad de la Información, de la República del Ecuador. Acuerdo Ministerial No. 005-2016.

Luego del diagnóstico realizado se considera pertinente plantear las siguientes acciones a ejecutar

PLAN DE SEGURIDAD DIGITAL [2020/2021]

como parte del Plan de Seguridad Digital durante el año **[2020/2021]**:

[Aquí va el plan, con la forma de un listado de temas cuyo orden puede variar según la importancia que tengan para la organización. Se trata básicamente de organizar la lluvia de ideas, no solo de incluir ideas nuevas, sino también de tratar aquellas que ya tienen identificadas, se sabe que tienen deficiencias o bien generan preocupación.

Idealmente las metas deben establecerse con tiempo suficiente para poder ver o seguir sus avances. Pueden tener el formato de una tabla, un cronograma o un simple listado.]

1. Incorporar costos de implementación en proyectos.
2. Implementar Sistema de Videoconferecia seguro.
3. Herramientas y técnicas para mejorar en la seguridad y en el rendimiento de la red institucional de la organización.
    a. Implementar un DNS sobre TLS seguro.
    b. Instalar un Proxy de Red.
    c. Evaluar la posible adquisición de una VPN institucional.
4. Implementar un Sistema de Gestión documental de bajo costo con las mejores funcionalidades disponibles.
    a. Evaluar distintas opciones de software libre (como NextCloud o Alfresco).
    b. Realizar un costeo de la implementación y mantenimiento.

i. Analizar la capacidad de almacenamiento actual y dispositivos de cómputo.

ii. Costos de almacenamiento.

iii. Costos de mantenimiento.

c. Implementar Sistema de Gestión Documental.

5. Implementar mejores prácticas en la gestión y mantenimiento de archivos.

a. Política y manual para el cifrado de equipos para protección de los activos de la información.

i. Realizar el cifrado de dispositivos móviles como tablets, celulares, etc.

ii. Realizar el cifrado de dispositivos de alma cenamiento externos como memorias flash, discos rígidos, etc.

b. Política y manual para comunicaciones seguras.

(entre muchas otras...)

Ejemplo de tabla:

Actividad	1° mes	2° mes	3° mes	4° mes	...
Incorporar costos de implementación en proyectos	X				
Implementar Sistema de Videoconferecia seguro	X				
Herramientas y técnicas para mejorar en la seguridad y en el rendimiento de la red institucional de la organización	X				
...					