

	SEGURIDAD BARRERA CTA	OP-P005
	INSTRUCTIVO – SEGURIDAD DE LA INFORMACIÓN	Versión: 001

1. CONSIDERACIONES INICIALES

Actualmente existe una dependencia cada vez mayor de las redes de computación para intercambio de información a través de diferentes tecnologías como el email, Intranet, etc. Con el libre flujo de la información y la gran disponibilidad de muchos recursos, las compañías tienen que conocer las potenciales amenazas que se ciernen sobre sus redes. Estas amenazas revisten muchas formas, pero todas ellas suponen una pérdida de la privacidad y la posible destrucción mal intencionada de la información o de los recursos, que puede llevar a grandes pérdidas económicas.

Conviene saber qué áreas de la red son más susceptibles a los intrusos y quiénes son los atacantes más habituales. La tendencia consiste en confiar en los usuarios internos de la red LAN y desconfiar de las conexiones que se originan en Internet o a través de módems de acceso telefónico y líneas dedicadas. Resulta importante confiar en los usuarios de la red y en el personal autorizado que utiliza los recursos internos de la red. La confianza también debe ser sopesada con la realidad. Es necesario restringir el uso de los equipos de la infraestructura de la red y los recursos vitales.

Cabe anotar que no todas las amenazas son maliciosas, pero pueden mostrar el mismo comportamiento y causar el mismo daño, independientemente de donde procedan. Es importante entender que tipos de ataques y puntos débiles son los más comunes y que hay que hacer a nivel normativo para garantizar un cierto grado de networking seguro.

2. TIPOS DE AMENAZA

Hay muchos tipos de amenazas, pero la mayoría de ellas se pueden englobar en tres categorías básicas:

- ✓ **Acceso no autorizado:** El acceso no autorizado tiene lugar cuando una entidad o individuo no autorizado consigue acceder a un activo y tiene la posibilidad de alterarlo. El acceso suele ser el fruto de la interceptación de información en tránsito sobre un canal inseguro o la explotación de un punto débil inherente a una tecnología o producto.
- ✓ **Suplantación de la identidad:** La suplantación de la identidad está íntimamente ligada al acceso no autorizado. Es la capacidad de presentar credenciales de alguien o algo que no se es. Estos ataques pueden adoptar varias formas: la apropiación de una clave privada, la obtención de acceso a un par nombre de usuario/contraseña.
- ✓ **Denegación de servicio:** La denegación de servicio (DoS) es una interrupción del servicio, bien debido a la destrucción del sistema, o bien debido a que temporalmente no está disponible. Entre los ejemplos más claros se incluye la destrucción del disco duro de un computador, los daños en la infraestructura física computacional y el uso de la memoria disponible en un recurso.

3. GESTION DE RIESGOS

La gestión de riesgos es una solución sistemática que sirve para determinar medidas de seguridad corporativas apropiadas. Cómo afrontar la seguridad, donde hacerlo y el nivel de controles de seguridad requiere una reflexión profunda. Antes de que las redes computacionales se generalicen, los datos confidenciales se conservaban bajo llave, y se suponía que la gente conservaba estos documentos en un lugar seguro en cajas de seguridad. En los entornos actuales este tipo de actividades han quedado obsoletas por razón de las redes de computadores. ¿Por qué tratar de ocultar una copia dura de un documento confidencial y sacarla de la oficina cuando se puede escanear, cifrar y enviar por correo electrónico? Las redes computacionales han creado un entorno en el que se puede acceder, trasladar o destruir electrónicamente los datos si no hay mecanismos electrónicos de bloqueo que protejan los secretos de la empresa. La gestión de riesgos comprende:

- 3.1. Identificación de los activos de la red: Es imposible saber quién puede ser el enemigo potencial de La Cooperativa. La Cooperativa de vigilancia comprende lo que desea proteger, que acceso es necesario para tales activos y como operan conjuntamente estas consideraciones. La Cooperativa está más preocupada de sus activos y valores asociados que de la motivación perseguida por un atacante. La Cooperativa identifica lo que requiere protección.

	SEGURIDAD BARRERA CTA	OP-P005
	INSTRUCTIVO – SEGURIDAD DE LA INFORMACIÓN	Versión: 001

A continuación, se enumeran los activos de red a tener en cuenta.

ACTIVO	DESCRIPCIÓN
HARDWARE	Estaciones de trabajo, computadores portátiles, impresoras, enrutadores, switches, módems, firewalls.
SOFTWARE	Programas fuente, programas de objeto, utilidades, programas de diagnóstico, sistemas operativos, programas de aplicación y programas de comunicación.
DATOS	Datos almacenados online y archivados offline, copias de seguridad, registros de auditoría, bases de datos y datos en tránsito sobre los medios de comunicación.
PERSONAS	Usuarios del sistema, administradores del sistema y mantenedores del hardware.
DOCUMENTACIÓN	Procedimientos, formularios, manuales e instructivos de procesos operativos y administrativos.

El inventario de los activos de La Cooperativa es dirigido conjuntamente con el fin de garantizar el manejo y la evaluación coherentes de los activos corporativos.

3.2. Clasificación de los datos: La clasificación de los datos en función de los distintos niveles de importancia puede ser un paso preliminar a la hora de establecer su valor. Un sistema sencillo de alto, medio y bajo puede ser el punto de partida que sirva para evaluar la importancia relativa de los datos. Los datos de La Cooperativa adoptan múltiples formas, entre las cuales se incluyen las siguientes:

- ✓ **Datos administrativos:** La correspondencia y otra información similar, como los registros y la información que este a disposición del público.
- ✓ **Datos financieros:** Información del presupuesto, de la contabilidad y en general relativa a los ingresos y gastos de las operaciones corporativas.
- ✓ **Datos del Cliente:** Información relacionada con el cliente que es de naturaleza personal o información desarrollada fruto de encuestas, entrevistas, auditorías, observaciones o recomendaciones.
- ✓ **Datos de investigación:** Información de apoyo de la actividad de investigación de una empresa.
- ✓ **Datos confidenciales:** Información que no puede ser revelada al público sin el permiso del propietario.

La siguiente tabla muestra cómo clasifican los distintos tipos de datos de La Cooperativa y aplica una clasificación en función de su importancia.

TIPO DE DATOS	CLASIFICACIÓN	IMPORTANCIA
Resultado de las Auditorías	Investigación	Alta
Estadísticas del Cliente	Investigación	Media
Memorandos Corporativos	Administrativo	Baja
Datos de Adquisición	Contabilidad	Alta
Secretos comerciales	Confidencial	Alta
Salario de los empleados	Contabilidad	Media

4. ELEMENTOS DE LA ARQUITECTURA DE SEGURIDAD

El marco global incluye los siguientes elementos de la arquitectura de seguridad de La Cooperativa:

	SEGURIDAD BARRERA CTA	OP-P005
	INSTRUCTIVO – SEGURIDAD DE LA INFORMACIÓN	Versión: 001

- ✓ **Identidad:** La identidad se define como el elemento de la arquitectura de seguridad que abarca la autenticación y la autorización. La autenticación responde a la pregunta ¿Quién es usted y dónde está? La autorización responde a la pregunta ¿A qué se le permite acceder? En necesario desplegar con precaución los mecanismos de identidad, ya que incluso las normas de seguridad más cuidadas pueden ser omitidas si las implementaciones son difíciles de usar. Un ejemplo clásico es el de las contraseñas garabateadas en una nota y pegados en el monitor del computador o en el teléfono (una solución real para el usuario que tenga que recordar muchas contraseñas) Otro ejemplo de seguridad mal implementada se da cuando los usuarios de la red utilizan una contraseña de fácil adivinación para no tener que escribirla: el nombre de un hijo, el nombre del perro, el nombre del esposo, el nombre de la esposa entre otros. La Cooperativa crea restricciones apropiadas dentro de sus sistemas, de forma que los intrusos que accedan a una parte del entorno corporativo, no tengan acceso automático al resto del entorno. Todos los computadores tienen activado el usuario de invitado con el cual se impide el acceso a la información confidencial.
- ✓ **Integridad:** La integridad es el elemento de la arquitectura de seguridad que abarca la seguridad de los dispositivos de la infraestructura de red (acceso físico y acceso lógico) y la seguridad del perímetro de red. El acceso físico a una computadora (o rotura, o switch o firewall) suele proporcionar a un usuario avezado un control total sobre este dispositivo. El acceso físico a una red suele permitir a una persona pulsar el enlace, bloquearlo o inyectar tráfico en él. Por lo tanto en la red LAN, la seguridad física deberá estar basada en control físico de acceso a personal no autorizado, circuitos cerrados de televisión y sistemas de acceso mediante claves encriptadas. Con estas medidas, La Cooperativa está segura de que en sus dependencias físicas, los activos están protegidos y que se mantiene una productividad de usuario alta. La seguridad del perímetro trata sobre la funcionalidad de tipo firewall, determinando que tráfico se permite o deniega en las distintas áreas de la red LAN. Los firewalls están colocados entre Internet y la red LAN.
- ✓ **Confidencialidad:** La confidencialidad es el elemento de la arquitectura de seguridad que garantiza la privacidad de la comunicación de los datos entre el remitente y el destinatario de la información. Unas normas de seguridad estrictas deberán dictar a los usuarios que tipo de información sensible deberán ir cifrados. Independientemente del nivel en que se dicten las normas, la decisión de usar el cifrado deberá ser tomada por la autoridad de la empresa que sea la responsable de garantizar la protección de la información sensible.
- ✓ **Disponibilidad:** La disponibilidad es el proceso de garantizar que todos los recursos vitales son accesibles. Mantener los datos disponibles significa que deberá haber una planificación de las actualizaciones del sistema y de los cambios en la configuración que estén probados para evitar sorpresas catastróficas causadas por errores o malas configuraciones del software.
- ✓ **Auditoría:** El elemento de auditoría de la arquitectura de seguridad es necesario para verificar y controlar las normas de seguridad corporativas. Una correcta auditoría verifica la implementación completa de las normas de seguridad en la infraestructura de la red LAN. El registro y el control subsiguiente de los eventos puede ayudar a detectar los comportamientos inusuales y las posibles intrusiones. Para probar la eficacia de la infraestructura de seguridad, la auditoría de seguridad deberá tener lugar frecuentemente y a intervalos regulares. La auditoría deberá incluir nuevas comprobaciones de la instalación del sistema, métodos para descubrir posibles actividades maliciosas de intrusos, la posible presencia de un tipo de problemas específico (ataque DoS) y el cumplimiento general de las normas de seguridad del sitio. Los rastros de auditoría suelen entrar en escena una vez que se sabe lo que ha ocurrido durante la evaluación del daño. Esta auditoría se hace cuando se actualiza la evaluación de riesgos de La Cooperativa de Vigilancia.

5. PROTECCION DEL ENTORNO

	SEGURIDAD BARRERA CTA	OP-P005
	INSTRUCTIVO – SEGURIDAD DE LA INFORMACIÓN	Versión: 001

La Cooperativa implementa protecciones del entorno apropiadas con el fin de proteger los recursos de red vitales. La importancia del sistema determina si la seguridad es o no adecuada. Cuanto más importante sea un sistema, más protecciones deberán implementarse para asegurar que el recurso está disponible a cualquier costo. La Cooperativa enfoca sus esfuerzos en garantizar las siguientes protecciones del entorno:

- Prevención, detección, supresión y protección contra incendios.
- Prevención, detección y control de inundaciones.
- Protección del suministro eléctrico.
- Control de la temperatura.
- Control de la humedad
- Protección frente a desastres naturales provocados por terremotos, rayos, tormentas etc.
- Protección frente a campos magnéticos excesivos
- Buenos procedimientos de limpieza para la protección contra la suciedad y el polvo.

6. PROTECCION DE LA AUTENTICACION

Es común encontrar en las empresas mecanismos de autenticación en contraseñas estándar y reutilizables. Cualquier contraseña reutilizable está expuesta a los ataques de escucha ilegal de programas sniffers (husmeadores). Conviene que en la medida de lo posible, estos entornos adopten un esquema de autenticación más sólido con respecto al manejo de las contraseñas.

A continuación, se enumeran algunas de las recomendaciones que da La Cooperativa a los trabajadores para el uso de las contraseñas tradicionales:

- ✓ Elija contraseñas que no se adivinen fácilmente. Muchos programas de detección automatizada de contraseñas utilizan un diccionario muy extenso y pueden descifrar contraseñas en cuestión de segundos.
- ✓ Cambie las contraseñas predeterminadas inmediatamente después de instalar equipos de infraestructura de red nuevo. Se deben cambiar las contraseñas para el acceso a la consola y las que se usan con fines de mantenimiento.
- ✓ La frecuencia con la que los usuarios deben cambiar su contraseña es como mínimo cada cuatro meses. Conviene cambiar las contraseñas cuando una cuenta con privilegios queda expuesta, o cuando haya un cambio crítico en el personal.

7. COMO ELEGIR LAS CONTRASEÑAS

A continuación, algunas directrices para elegir las contraseñas apropiadas:

- ✓ No utilice el nombre de inicio de sesión arbitrariamente (tal como es, invertido, en mayúsculas, duplicado, etc.)
- ✓ No utilice el nombre o el apellido arbitrariamente
- ✓ No utilice los nombres de parientes muy próximos o los nombres de personas o animales muy allegados. (Esposa, esposo, novia, padre, mascotas, etc.)
- ✓ No emplee otra información relativa a su persona o pertenencias que se obtenga de manera sencilla, como los números de matrícula del carro, los números de teléfono, la marca del carro que conduce, el nombre de la calle donde vive, etc.
- ✓ No utilice una contraseña de todos dígitos o que tenga toda ella las mismas letras. Este tipo de contraseñas reduce el tiempo de búsqueda de un atacante.
- ✓ No utilice una palabra que se incluya en los diccionarios de inglés, de español o cualquier idioma, listas ortográficas u otra lista de palabras.
- ✓ No emplee una contraseña que tenga menos de seis caracteres.

	SEGURIDAD BARRERA CTA	OP-P005
	INSTRUCTIVO – SEGURIDAD DE LA INFORMACIÓN	Versión: 001

- ✓ No revele nunca su contraseña de red. La protección de la contraseña es su responsabilidad.
- ✓ La finalidad última de que haya una contraseña consiste en asegurarse de que nadie (que no sea usted) pueda usar sus inicios de sesión. Recuerde que los secretos mejor guardados son los que se guardan para uno mismo.
- ✓ No envíe por correo electrónico su contraseña.
- ✓ Utilice siempre una contraseña que incluya caracteres no alfabéticos, como dígitos o signos de puntuación.
- ✓ Utilice una contraseña que sea fácil de recordar, ya que conviene no anotarla.
- ✓ Utilice una contraseña que pueda escribir rápidamente sin tener que mirar el teclado. Esto hará que sea más difícil que alguien se apropie de su contraseña. Cuídese de escribir contraseñas delante de los demás.
- ✓ Cambie su contraseña periódicamente. Trate de cambiarla cada cuatro meses.

8. NORMAS Y PROCEDIMIENTOS PARA EL PERSONAL

Las personas encargadas de mantener y actualizar la infraestructura de red deberán tener directrices específicas que les ayuden a desempeñar sus tareas con arreglo a las normas de seguridad corporativas.

9. COPIAS DE SEGURIDAD

El procedimiento para la creación de copias de seguridad constituye una parte integral de la ejecución de un entorno computacional. La siguiente lista muestra las normas de copia de seguridad a seguir:

- ✓ Asegúrese de que su sitio está creando copias de seguridad para todas las configuraciones e imágenes de software del equipo de la infraestructura de red.
- ✓ Asegúrese de que su sitio está creando copias de seguridad para todos los servidores que proporcionen servicios de red.
- ✓ Asegúrese de que su sitio está almacenando fuera del sitio las copias de seguridad. El sitio de almacenamiento deberá seleccionarse cuidadosamente en aras de la seguridad y disponibilidad.
- ✓ Cifre sus copias de seguridad para proporcionar una protección adicional a la información cuando esta fuera del sitio.
- ✓ No presuponga que las copias de seguridad siempre son buenas.
- ✓ De forma periódica, verifique el estado y la corrección de sus copias de seguridad.

La Cooperativa realiza copias de seguridad de todos sus equipos cada dos meses, dejando una copia en la caja fuerte de la empresa y una fuera de las instalaciones en poder del gerente general.

10. USO DE EQUIPOS Y HERRAMIENTAS PORTATILES

Los equipos portátiles plantean riesgos. Debe asegurarse de que el robo de alguno de los equipos portátiles de un miembro del personal no va a causar problemas. Se deben desarrollar directrices para los tipos de datos que residen en los discos duros de los portátiles, así como para la protección de los datos (por ejemplo, si se debe utilizar o no el cifrado) cuando se trate de una computadora portátil.

11. INGENIERIA SOCIAL

Muchos intrusos tienen más éxito utilizando la ingeniería social que con la piratería técnica. Una de las normas de formación más importantes es que los empleados y los usuarios no deben creer a cualquiera que llame por teléfono y les pregunte por algo que pueda poner en peligro la seguridad. ¿Por qué revelar al interlocutor información financiera personal y aceptar una

	SEGURIDAD BARRERA CTA	OP-P005
	INSTRUCTIVO – SEGURIDAD DE LA INFORMACIÓN	Versión: 001

nueva contraseña por teléfono? Esto no puede ser así, ya que no se ha establecido la identidad del interlocutor. Lo mismo es aplicable a las contraseñas y a la información corporativa confidencial solicitada por teléfono. Antes de divulgar información confidencial, deberá identificar positivamente a la persona con la que se está hablando.

12. CONCLUSIONES

Para ser eficaces, los procedimientos de seguridad informática deberán ser concisos e ir al grano. Deberán abarcar reglas que definan los controles de seguridad física (que pertenecen a la infraestructura física, a la seguridad de los dispositivos físicos y al acceso físico) Entre estas reglas se deberán incluir directrices que protejan la integridad y confidencialidad de los datos con el fin de garantizar que tales datos no han sido alterados durante el tránsito y que solo son entendibles por el emisor y el destinatario de la información. La Cooperativa de Vigilancia proporciona a los empleados formación apropiada que les instruyan acerca de los potenciales problemas relacionados con la seguridad informática.

CONTROL DE CAMBIOS

FECHA DEL CAMBIO	VERSIÓN	DESCRIPCIÓN DEL CAMBIO

REVISIÓN Y APROBACIÓN

SANTIAGO ARIAS	DANIELA HIGUITA USUGA
REALIZA: GESTOR HSEQ	REVISY Y APRUEBA: GERENCIA