GUÍA DE SEGURIDAD DE LAS TIC
(CCN-STIC-814)

SEGURIDAD EN CORREO ELECTRÓNICO

AGOSTO 2011

Edita:

NIPO: 075-11-053-3
Tirada: 1000 ejemplares
Fecha de Edición: agosto de 2011
S2 Grupo y Antonio Villanlón Huerta han elaborado el presente documento y sus anexos.
El Ministerio de Política Territorial y Administración Pública ha financiado el desarrollo del presente documento y sus anexos.

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el **Centro Criptológico Nacional** puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia de la serie de documentos CCN-STIC.

Disponer de un marco de referencia que establezca las condiciones necesarias de confianza en el uso de los medios electrónicos es, además, uno de los principios que establece la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 sobre el Esquema Nacional de Seguridad (ENS).

Precisamente el Real Decreto 3/2010 de 8 de Enero de desarrollo del Esquema Nacional de Seguridad fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Agosto de 2011

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

ANEXOS

1. INTRODUCCIÓN

1.1. CONCEPTOS PREVIOS

1. El correo electrónico es hoy en día uno de los mecanismos de intercambio de información más utilizados, tanto en el ámbito personal como en el profesional. Todas las personas que utilizan Internet en su trabajo o en su hogar disponen de una o más cuentas de correo electrónico, cuentas que, como veremos más adelante, sufren a diario ataques de todo tipo con el objetivo principal de robar información.

2. El envío de correo electrónico es, desde el punto de vista del usuario, un proceso completamente transparente: escribimos un mensaje, rellenando unos campos concretos (como el receptor o el asunto) y lo enviamos desde un cliente concreto, apareciendo al poco tiempo el mensaje en el buzón de su destinatario. No obstante, este proceso, como hemos dicho transparente para el usuario, lleva asociados una serie de elementos tecnológicos y de protocolos de transporte y acceso que es necesario conocer para poder hablar de la seguridad en el correo electrónico; vamos a describirlas, al menos a nivel introductorio, en el punto siguiente.

3. Para resumir el proceso habitual[1] de envío y recepción de un mensaje de correo electrónico, cuando el emisor compone el mensaje indicando los campos habituales (dirección destino, asunto, cuerpo…), su cliente de correo se encarga de enviarlo al servidor de correo predeterminado (habitualmente, el servidor corporativo de la organización). Éste, al recibir el correo, realiza una serie de comprobaciones técnicas (el contenido está correctamente formado, existe una dirección destino, el usuario está autorizado…) y, si son correctas, envía el mensaje al servidor destino, que lo procesa y almacena en el buzón del usuario al que va dirigido el correo para que éste pueda proceder a su lectura.

4. Desde un punto de vista técnico y de seguridad, podemos diferenciar dos partes en un correo electrónico: el cuerpo y las cabeceras. La primera está formado por el contenido del mensaje en sí (incluyendo posibles adjuntos, previamente tratados para poderse transmitir), y por tanto depende por completo de lo que el usuario haya decidido incluir en dicho mensaje. La segunda parte a la que hacíamos referencia, las cabeceras, contiene información tanto facilitada de una u otra forma por el usuario (asunto, destinatario, emisor…) como añadida por el servidor o servidores por los que pasa el mensaje hasta llegar a su destino.

5. Estas cabeceras son importantes para determinar algunos aspectos de seguridad de los correos electrónicos; en especial para conocer el camino que un mensaje ha seguido entre emisor y receptor, ya que cada vez que el mensaje pasa por un servidor de correo éste añade un campo de datos a las cabeceras, con etiqueta *Received*, especificándose el nombre del servidor, su dirección IP, el servidor de correo utilizado, y la fecha y la hora en que se recibió el mensaje. De esta forma podemos determinar si un correo proveniente de un cierto dominio de Internet se ha procesado efectivamente en servidores relacionados con dicho dominio o por el contrario viene de sistemas que a priori no son propios del mismo, lo que indicaría que el mensaje puede haber sido falseado.

[1] Existen variantes a este modelo que quedan fuera del ámbito de la presente guía.

1.2. TECNOLOGÍAS IMPLICADAS

6. En el presente punto se describen algunas de las tecnologías implicadas en la gestión del correo electrónico, desde que el emisor compone un mensaje hasta que el receptor lo procesa (lectura, borrado, reenvío…). No es objeto de la presente guía ni una descripción detallada de cada uno de los protocolos o elementos involucrados ni una relación exhaustiva de tecnologías implicadas en la gestión de correo, remitiendo para ello al lector a publicaciones especializadas en la materia, sino una descripción breve y no técnica de los elementos que intervienen habitualmente en el envío y recepción de un correo electrónico.

1.2.1. PROTOCOLOS DE TRANSPORTE

1.2.1.1. SMTP

7. SMTP (Simple Mail Transfer Protocol) es, como su nombre indica, un protocolo de comunicaciones para el transporte y entrega del correo electrónico; se trata del protocolo estándar para intercambio de mensajes, por lo que cualquier servidor de correo que desee recibir e-mail en términos generales, deberá ser capaz de "entender" SMTP.

8. Cuando el usuario compone un correo electrónico, su cliente de correo (MUA, como veremos a continuación) debe conectarse al servidor de correo corporativo (MTA) –el que va a utilizarse para enviar el mensaje- y, mediante el protocolo SMTP, indicarle los parámetros necesarios para procesar dicho mensaje (a quién va dirigido, quién lo envía, cuál es el cuerpo, etc.). Si la negociación es correcta, el servidor recogerá el mensaje y se encargará, a su vez, de transmitirlo a otro servidor de correo, posiblemente el gestor del dominio de correo al que va dirigido dicho mensaje. Este proceso es transparente para el usuario, ya que la negociación con el MTA la realiza el cliente de correo; no obstante, podríamos simular esta negociación mediante un cliente telnet y las órdenes SMTP adecuadas, tal y como se muestra a continuación –de forma simplificada-:

```
$ telnet mta 25
Trying 192.168.1.51...
Connected to mta.
Escape character is '^]'.
220 mta ESMTP Service (Lotus Domino Release 9.0.0) ready at Mon,
11 Jul 2011   03:53:30 +0200
helo aaa
250 mta Hello aaa ([172.17.0.14]), pleased to meet you
mail from: test@dominio.es
250 test@dominio.es... Sender OK
rcpt to: test@organismo.es
250 test@organismo.es... Recipient OK
data
354 Enter message, end with "." on a line by itself
```

```
Cuerpo del mensaje
.
250 Message accepted for delivery
quit
221 mta SMTP Service closing transmission channel
Connection closed by foreign host.
$
```

1.2.1.2. ESMTP

9. A medida que el número de usuarios de correo electrónico ha ido creciendo y las funcionalidades en los entornos de correo se han ampliado, se ha hecho necesaria la extensión del protocolo SMTP –muy básico- para incluir nuevas capacidades en el mismo, dando lugar a ESMTP o SMTP Extendido. Estas nuevas capacidades del protocolo son nuevas órdenes SMTP, extensiones del servicio SMTP y parámetros adicionales para órdenes del protocolo clásico, cuya descripción exhaustiva queda fuera del ámbito de la presente guía.

10. La mayor parte de servidores de correo utilizados en la actualidad proporcionan a sus usuarios capacidades SMTP extendidas, siendo siempre compatibles con el protocolo SMTP original; los administradores de sistemas de correo electrónico deben revisar las extensiones habilitadas en sus servidores, en especial las relativas a autenticación de usuarios o transporte seguro de datos para que en caso de necesitar la utilización de alguna de ellas, y siempre que técnicamente sea posible, se incorporen correctamente al entorno de correo corporativo.

1.2.2. PROTOCOLOS DE ACCESO

11. Cuando un correo electrónico llega al buzón de su destinatario, éste necesita acceder al mismo para poder procesar el mensaje; en ciertos entornos –típicamente sistemas Unix-, el acceso al buzón se realiza en modo local, esto es, el usuario se autentica en el sistema mediante su contraseña y, una vez en línea de órdenes, puede ejecutar un cliente del sistema (pine, elm, mail…) para procesar el correo electrónico. Obviamente, esto requiere de un acceso válido al sistema en modo línea de órdenes –o un shell restringido con acceso al cliente de correo-, lo que tiene implicaciones desde el punto de vista de seguridad: los usuarios podrían explotar, con relativa facilidad, fallos locales en el sistema para conseguir acceso privilegiado al mismo. Por este motivo, y también por aspectos de funcionalidad (los usuarios no suelen estar familiarizados con el entorno de órdenes Unix), esta aproximación básica es cada vez menos utilizada, habiendo sido sustituida por accesos desde el equipo de usuario directamente a los buzones de correo a través de un cliente o de un navegador web.

12. Para poder realizar el acceso directo a los buzones de correo se desarrollaron protocolos concretos, principalmente POP3 e IMAP, y sus equivalentes seguros; desde el equipo de usuario, con un cliente adecuado y mediante estos protocolos, el usuario es capaz de procesar su correo electrónico sin necesidad de acceso en línea de órdenes al servidor.

Adicionalmente, se utiliza cada vez más el acceso al correo mediante un navegador, lo que se conoce como *webmail*, aspecto que también describiremos en este punto.

1.2.2.1. POP3

13. POP3 (*Post Office Protocol version 3*) es un protocolo que permite descargar mensajes desde el servidor de correo hacia un equipo de usuario, desde el que se inicia la conversación y que, tras autenticarse convenientemente, pasa a recibir el contenido del buzón albergado en el servidor, borrando –habitualmente- el contenido del mismo. Este es quizás el protocolo más utilizado en muchos entornos, en los que los usuarios, con clientes como Icedove o Microsoft Outlook, descargan su correo al equipo local y lo procesan adecuadamente.

14. POP3 presenta problemas asociados al borrado del correo en el servidor, tras la descarga por parte del usuario; cuando se descarga el contenido de un buzón, típicamente se elimina del servidor, lo que implica que a partir de ese momento el usuario es el único responsable de la custodia de los mensajes, por ejemplo en temas de copia de seguridad de los mismos. Adicionalmente, si se utilizan diferentes equipos para la descarga, el correo del usuario puede acabar disperso entre todos ellos, con los riesgos de funcionalidad y de seguridad que esto implica.

15. El usuario puede configurar su cuenta POP3 para que no se eliminen los correos al ser descargados desde un cliente, lo que mitiga buena parte de los problemas descritos con anterioridad. No obstante, si se utiliza esta configuración, cada vez que se descargue el correo desde un nuevo cliente (por ejemplo tras una reinstalación de equipo o para consultar el e-mail en otro puesto) se descargará de nuevo todo el contenido del buzón, ya que este reside por completo en el servidor.

1.2.2.2. IMAP

16. Para eliminar alguno de los problemas descritos con anterioridad se diseñó el protocolo IMAP (*Internet Message Access Protocol*), que permite básicamente que los buzones de correo de los usuarios se encuentren centralizados en el servidor de correo y por tanto puedan ser accedidos con la misma visión de éstos desde diferentes clientes.

17. Desde un punto de vista de seguridad, el uso de IMAP es preferible al de POP3; no obstante, aquí encontramos un problema de la capacidad, ya que el servidor de correo deberá disponer de un sistema de almacenamiento de capacidad adecuada para hospedar los buzones de todos los usuarios; dada la cantidad de información remitida por correo electrónico, el entorno de almacenamiento puede convertirse en un problema por el espacio en disco requerido para todos los buzones de los usuarios.

18. Una aproximación que permite minimizar en parte el problema anterior es el uso de IMAP con políticas de archivado concretas: los mensajes que cumplan ciertas condiciones, típicamente temporales, se almacenarán *offsite*, dejando de ocupar espacio de almacenamiento primario en el servidor de correo y pasando a cintas, repositorios, etc.

1.2.2.3. Webmail

19. Es cada vez más habitual el acceso al correo, tanto personal como corporativo, a través de un navegador web, lo que se conoce como *webmail* o correo web. Estos accesos se realizan a través de protocolo HTTPS (es obligatorio el uso de protocolo seguro, jamás debemos utilizar el protocolo HTTP para acceder al correo electrónico) contra una determinada dirección y, tras autenticarnos convenientemente a través del interfaz web, se muestra al usuario el contenido de sus carpetas de correo y las diferentes opciones de gestión del mismo (envío, borrado, archivado…).

20. Desde un punto de vista técnico, un webmail no es más que un entorno de gestión de mensajes de correo a través de web; los protocolos de transporte, tecnologías implicadas, etc. son los mismos que con el uso de MUA tradicionales, con la diferencia de que estos elementos se utilizan entre el servidor de correo y el servidor web, no entre el MUA y el MTA, y el navegador, a través de aplicaciones web, nos proporciona las capacidades de gestión de mensajes de cualquier cliente nativo.

1.2.3. SISTEMAS IMPLICADOS

1.2.3.1. MUA

21. Se denomina MUA (*Mail User Agent*) al cliente de correo electrónico desde el que el usuario gestiona los mensajes: creación, borrado, envío, lectura… Habitualmente, se utiliza para un MUA para enviar correo electrónico, a través del MTA correspondiente (ver punto siguiente) y mediante el protocolo SMTP o sus extensiones, así como para recibir correo electrónico, también desde el MTA correspondiente y mediante protocolos como POP3 o IMAP.

22. Ejemplos habituales de MUA son Mozilla Thunderbird, Microsoft Outlook, Eudora, KMail o Evolution; todos ellos permiten la gestión del correo electrónico corporativo mediante los protocolos habituales, aunque por motivos de compatibilidad y funcionalidad, es necesario que en cada organización se analice la conveniencia de utilizar un MUA como estándar para todo el personal, siempre que técnica y organizativamente sea factible.

1.2.3.2. MTA

23. Se denomina MTA (*Mail Transfer Agent*) al sistema implantado en el servidor de correo capaz de recibir mensajes desde un MUA, procesarlos convenientemente y entregarlos a sus destinatarios mediante uno o más protocolos de comunicación. Típicamente, el MTA debe ser capaz de comunicarse mediante el protocolo SMTP –o sus extensiones- para enviar y recibir correos y, adicionalmente, suelen comunicarse mediante POP3 o IMAP para que los usuarios puedan gestionar sus buzones de correo.

24. Ejemplos habituales de MTA son sendmail, qmail, posftix o exim en entornos Unix, Microsoft Exchange sobre entornos Windows y Lotus Domino en multiplataforma (estos últimos sistemas incorporan, aparte de la capacidad de MTA, características adicionales y protocolos propietarios diferentes en cada caso, obviamente fuera del alcance de la presente guía).

1.3. RIESGOS ASOCIADOS AL CORREO ELECTRÓNICO

25. Nadie duda de la revolución que el correo electrónico ha supuesto a la hora de trabajar en cualquier organismo, introduciendo innumerables ventajas de entre las que destaca la rapidez de comunicación y envío de datos; pero como cualquier cambio, el correo electrónico introduce una serie de riesgos que es necesario conocer y, hasta donde sea posible, mitigar, para garantizar la confidencialidad, integridad y disponibilidad de la información corporativa. Por este motivo, el Esquema Nacional de Seguridad introduce medidas de seguridad relativas a los servicios de correo electrónico ([mp.s.1]) que, con independencia de la categoría del sistema, especifica la obligatoriedad de proteger la información transmitida tanto en el cuerpo como en los anexos de un mensaje, de proteger la información de encaminamiento y establecimiento de conexiones y de proteger a la organización frente a las amenazas especialmente vinculadas al correo electrónico, como el spam, el software dañino o el código móvil.

26. La organización debe ejecutar un análisis de riesgos que evalúe amenazas, probabilidades, impactos, riesgos efectivos, salvaguardas y riesgos residuales que afecten a los sistemas corporativos de correo electrónico, en función de su categoría y siguiendo las directrices definidas en el ENS ([op.pl.1]); dicho análisis suele y puede estar contenido en un análisis global de riesgos para la organización, y permitirá conocer los principales riesgos a los que está expuesto el correo corporativo y las salvaguardas aplicadas para mitigarlos. Vamos a describir en este punto, sin tratar de presentar una relación exhaustiva, algunos de dichos riesgos.

1.3.1. SOFTWARE DAÑINO

27. El correo electrónico es un medio ideal para la propagación de software dañino, conocido como malware, a través de Internet. La rápida difusión de los mensajes, incluso sin intervención directa del usuario emisor, hace que cualquier tipo de malware enviado a través del correo electrónico pueda llegar en pocas horas a miles de usuarios, potenciales víctimas de dicho malware.

28. Para evitar la contaminación del receptor de un correo electrónico es necesario la utilización de sistemas antivirus, tanto en el equipo donde se lee el mensaje como en servidores de correo intermedios, así como un uso correcto del correo electrónico por parte del usuario: no ejecutar archivos adjuntos, no confiar en correos de destinatarios desconocidos (o conocidos que puedan ser sospechosos de haber sido falsificados), etc., tal y como veremos en los apartados correspondientes de la presente guía.

1.3.2. SPAM

29. Bajo la denominación SPAM se identifica el correo no deseado por el usuario, tanto publicitario como contenedor de ataques más severos a la seguridad de la información. Habitualmente el SPAM trata de ofrecer servicios fraudulentos, como la compra de productos falsificados o por debajo de su precio de coste (típicamente, medicamentos o artículos de lujo), pero bajo la etiqueta de correo no deseado es también común recibir ataques de phising; estos ataques consisten en el envío de correos con un origen aparentemente fiable (en general, entidades bancarias, aunque también han sufrido ataques de phishing otro tipo de servicios, como los ofrecidos por la Agencia Tributaria) pero que, mediante enlaces en el cuerpo del correo electrónico que dirigen al usuario a

páginas web falsificadas, intenta obtener datos confidenciales de su víctima (habitualmente, credenciales de acceso a banca online)-.

1.3.3. FUGAS DE INFORMACIÓN

30. El correo electrónico es una potencial fuente de fugas de información, ya que permite remitir volúmenes relativamente importantes de datos a un tercero de una forma que no siempre es posible detectar; adicionalmente, si consideramos la facilidad con la que habitualmente los usuarios pueden acceder a correos externos a la organización –en especial, a través de web-, nos encontramos ante un punto de fuga de datos a considerar a la hora de implantar controles. Puede ser sencillo monitorizar el sistema de correo corporativo para detectar envíos de correos electrónicos de gran tamaño a direcciones ajenas a la organización (aunque el volumen de alertas generadas será muy considerable), pero la monitorización de correos externos es siempre complicada.

1.3.4. INGENIERÍA SOCIAL

31. El correo electrónico puede convertirse en una herramienta utilizada contra la organización para ejecutar ataques de ingeniería social. Dichos ataques suelen tener como objetivo usuarios concretos que bien por su trabajo, bien por su nivel de privilegios en la red, pueden facilitar al atacante datos relevantes sin ellos saberlo, derivando en problemas de fugas de información, malware, etc. como los indicados con anterioridad.

1.3.5. DAÑOS A LA IMAGEN

32. El uso del correo corporativo de forma que se degrade la imagen de la organización no es habitual, pero debemos tener en cuenta que un uso inadecuado de las direcciones de correo electrónico propias de una organización puede perjudicar seriamente a su imagen: si un usuario envía correos insultantes, de contenido ilícito, que fomenten actitudes contrarias a la convivencia… no sólo se perjudicará la imagen de esta persona, sino la de la organización en su conjunto; de esta forma, nuestra política de uso del correo electrónico debe reflejar claramente la prohibición del uso del correo corporativo con estos fines, minimizando así tanto la probabilidad como el impacto asociados al riesgo reputacional en el uso del correo.

1.3.6. BULOS

33. El correo electrónico es un medio habitual de propagación de bulos (*hoaxes*), noticias falsas que intentan pasar por reales ante sus receptores; a diferencia de los fraudes, como el phishing, los bulos no tienen por qué tener propósito delictivo o de lucro, aunque pueden implicar impactos muy dañinos contra una organización. El envío de un *hoax* puede ser el medio para cometer un ataque de ingeniería social, de envío de software dañino, de recopilación de direcciones de correo electrónico o incluso un ataque semántico severo contra una determinada entidad. En cualquier caso, con independencia de su fin último, el procesamiento de los bulos debe considerarse un riesgo potencial para la seguridad corporativa.

34. Es imposible detener el envío de bulos mediante mecanismos técnicos en exclusiva; las salvaguardas tecnológicas pueden reducir el riesgo, pero desde un punto de vista técnico

los bulos se transmiten de forma lícita a través del correo electrónico: para el sistema de correo se trata de mensajes legítimos enviados desde direcciones correctas propias o ajenas a la organización. Al tratarse de ataques semánticos, no sintácticos, la única forma de mitigarlos satisfactoriamente es mediante una correcta formación ([mp.per.4]) y concienciación ([mp.per.3]) de los usuarios de la organización, por lo que es obligatorio incluir estos controles en todos los casos, proporcionando a los usuarios directrices para detectar los bulos que reciben a través del correo electrónico.

1.4. POLÍTICAS DE USO DEL CORREO ELECTRÓNICO

35. Las organizaciones deben regular formalmente, entre otros, el uso del correo electrónico corporativo por parte de sus empleados; habitualmente esta regulación no se recoge en una política de seguridad corporativa ([org.1]), sino en forma de normativa específica sobre el uso del correo electrónico en la organización ([org.2]).

36. La regulación del uso del correo electrónico debe contener obligatoriamente, sin menoscabo de otros cualesquiera, los siguientes extremos en cuanto a deberes y obligaciones de su uso ([mp.per.2]):

37. Uso adecuado, racional y leal del correo electrónico corporativo, en especial en lo relativo a la confidencialidad de los datos.

38. Regulación del envío de información sensible o de datos de carácter personal a través del correo electrónico.

39. Prohibición expresa del uso del correo corporativo con fines personales, con la posible excepción del uso razonable del mismo siempre que éste no introduzca riesgos significativos en la organización.

40. Garantía reputacional. Prohibición expresa del uso del correo electrónico corporativo en cualquier forma que degrade o pueda degradar la reputación de la organización o de las personas que la componen (mensajes sexistas, racistas, xenófobos…).

41. Directrices de almacenamiento y eliminación del correo en servidores corporativos.

42. Directrices de actuación ante correos electrónicos recibidos por el usuario que puedan suponer un riesgo para la seguridad de la organización.

43. Medidas disciplinarias a que haya lugar en caso de incumplimientos de los deberes y obligaciones en el uso del correo electrónico.

44. En el anexo correspondiente de la presente guía se muestra un ejemplo de normativa de uso del correo electrónico, normativa que debemos adaptar a nuestra organización para recoger en la misma sus particularidades, notificar formalmente a los empleados –incluso obteniendo su conformidad mediante firma- y aplicar convenientemente, incluyendo controles técnicos que fuercen directrices siempre que ello sea posible.

45. Adicionalmente a la regulación corporativa del uso del correo electrónico y por supuesto a cualquier control técnico, la organización debe evaluar la conveniencia de facilitar al personal recomendaciones o restricciones directas en dicha utilización; estas directrices se considerarán siempre dependientes de la regulación anterior, y tienen como objetivo la mayor concienciación del personal en temas referentes a la seguridad en el uso del correo electrónico ([mp.per.3]). Son de especial las referentes a:

46. Prohibición de ejecución de ficheros adjuntos provenientes de fuentes no confiables.

47. Prohibición de envío de información sensible fuera de las premisas de la organización sin cumplir las medidas de seguridad oportunas.

48. Prohibición de respuesta a cualquier mensaje considerado sospechoso, incluyendo los mensajes de SPAM que requieren de un correo para dar de baja la dirección de una lista de distribución concreta.

49. Restricción en el uso de correos personales para envío de información sensible.

50. Recomendaciones para identificar ataques de phishing contra la organización.

51. El equipo de seguridad debe ser consciente de la importancia de la concienciación de los usuarios, punto débil habitual en cualquier esquema de seguridad, y por tanto lanzar las iniciativas adecuadas para conseguir que las personas sean parte activa de la seguridad corporativa, en este caso en los aspectos referentes al uso del correo electrónico.

1.5. CONSIDERACIONES ORGANIZATIVAS

52. A la hora de implantar una solución de correo seguro ([op.pl.3]), cada organización debe analizar formalmente sus requisitos de seguridad (incluyendo restricciones legales), plasmados probablemente en la política de uso del correo electrónico corporativo, y planificar la implantación eligiendo un producto o servicio acorde a dichos requisitos, en especial a las conclusiones del análisis de riesgos. Habitualmente se incorporará un sistema que proporcione diferentes capacidades de seguridad (cifrado y firma de datos, antivirus, antispam…) y para su elección, así como para garantizar el éxito de la iniciativa y la seguridad efectiva del correo, deben tenerse en cuenta los siguientes factores, sin menoscabo de otros cualesquiera a considerar por la organización:

53. **Cifrado.** El sistema debe proporcionar cifrado robusto y basado en estándares internacionales.

54. **Tránsito de datos.** Si en la solución se produce tránsito de datos en texto claro, por ejemplo en arquitecturas Boundary to Boundary o en servicios de correo web, es necesario garantizar que dicho tránsito no afecta a la confidencialidad de la información corporativa y que se cumplen las restricciones legales de aplicación, en especial las relativas a datos de carácter personal.

55. **Costes.** La implantación de un sistema de correo seguro determinado puede suponer para la organización un cierto coste –tanto directo como indirecto-, por lo que es necesario analizar en términos económicos diferentes alternativas y aplicar la más adecuada en cada caso. El factor coste no debe anteponerse bajo ninguna condición al factor seguridad.

56. **Facilidad de uso.** La solución implantada debe ser sencilla en su uso diario, al menos de forma relativa; si el sobrecoste de utilización de un modelo de correo seguro es elevado o el usuario requiere de conocimientos técnicos para su uso, probablemente acabe desechada, o simplemente los usuarios utilizarán mecanismos alternativos, fuera del control de seguridad de la organización, para intercambiar datos.

57. **Capacidad de integración.** La solución a implantar debe integrarse todo lo posible tanto con las arquitecturas (red, hardware, software…) existentes en la organización como con el usuario, sus capacidades y sus necesidades. Debemos considerar cuidadosamente soluciones que obliguen a grandes modificaciones en el entorno, que no se integren con los elementos preexistentes (incluyendo clientes de correo) o que requieran de un gran número de recursos computacionales para la gestión de un simple correo.

58. **Monitorización.** La solución elegida, bien de forma directa bien a través de mecanismos indirectos, debe generar los registros correspondientes y disponer de capacidad de alerta ante situaciones anómalas que puedan repercutir en la seguridad de la información corporativa: intentos de acceso no autorizados, funcionamientos incorrectos, anomalías en el uso del sistema…

1.6. ROLES EN LA SEGURIDAD DEL CORREO ELECTRÓNICO

59. Tal y como se ha indicado con anterioridad, garantizar la seguridad del correo electrónico es vital en cualquier organización, ya que este medio se utiliza a diario para el envío de información sensible de la que interesa preservar características como la confidencialidad, integridad o no repudio. De esta forma, las organizaciones deben maximizar los controles de seguridad en los sistemas de correo corporativos, y un aspecto clave para ello es la **separación de tareas** en los entornos de correo electrónico, como un medio para prevenir o mitigar el riesgo asociado a errores, vulnerabilidades o compromisos de seguridad en general.

60. Cada organización debe evaluar un esquema de seguridad que proporcione control dual en el entorno de correo electrónico corporativo; independientemente del esquema escogido, deben reflejarse al menos los siguientes roles:

61. **Administradores de sistemas.** Su función es garantizar la seguridad y funcionalidad de los sistemas y aplicaciones implicados en la gestión del correo electrónico corporativo, incluyendo la información almacenada, tratada, enviada o recibida por los mismos. Este rol recae habitualmente en departamentos de sistemas.

62. **Administradores de redes.** Su función es garantizar la seguridad de la información en tránsito en las redes corporativas. Este rol recae habitualmente en departamentos de comunicaciones.

63. **Administradores de seguridad.** Su función es garantizar la seguridad de la información corporativa en su conjunto, con independencia absoluta –incluyendo línea de mando- de los roles anteriores, definiendo directrices de seguridad para la organización y velando por su correcto cumplimiento, derecho de auditoría incluido. Este rol recae habitualmente en departamentos de seguridad corporativa, auditoría o control interno.

64. Definir estos roles debe garantizar que las acciones del personal con acceso directo a la información gestionada en los entornos de correo o transmitida por la red de comunicaciones corporativa, que por su trabajo requerirá habitualmente de privilegios en dichos entornos, son controladas y auditadas de forma correcta, minimizando así el riesgo de fraudes o fugas de información.

65. El planteamiento de al menos estos tres roles es un mínimo expuesto a organizaciones de todo tipo; por supuesto, cada organización debe evaluar, en función de su tamaño o restricciones de seguridad, complementar los roles anteriores con figuras adicionales que mejoren el proceso de seguridad no sólo en el correo electrónico, sino en la organización en general.

2. SEGURIDAD DEL SERVIDOR DE CORREO

2.1. ARQUITECTURA DE RED

66. El servidor de correo electrónico corporativo debe estar ubicado en una zona desmilitarizada (DMZ); dicha zona de red es el segmento en el que la organización ubica los sistemas que están ofreciendo servicios a Internet (no sólo el correo electrónico), y debe estar aislado tanto de Internet como de la red interna de la organización mediante un cortafuegos correctamente configurado, que permita únicamente los tráficos estrictamente necesarios para el correcto funcionamiento de los sistemas y servicios corporativos ([mp.com.4]). Esta arquitectura es la que menor riesgo introduce en la seguridad de la organización y es obligatoria en entornos de categoría ALTA, ya que ubicar los sistemas de correo en una zona interna implicaría que un problema de seguridad en dichos sistemas podría afectar directamente a los servidores internos de la organización (arquitecturas alternativas, como la ubicación del servidor de correo electrónico delante de los cortafuegos corporativos, no se contemplan por motivos obvios de seguridad).

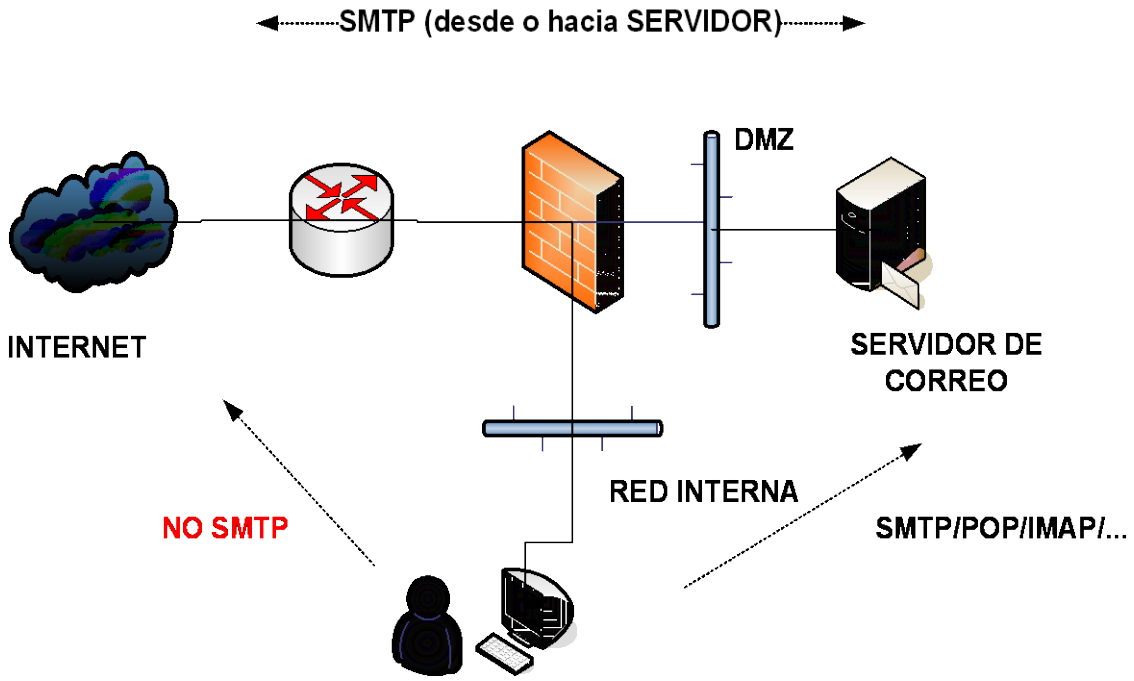
67. La organización debe evaluar cómo configurar su zona desmilitarizada en la red en función de sus requisitos de seguridad y necesidades operativas. Habitualmente, existen dos aproximaciones; en la primera de ellas la DMZ corporativa se configura con dos elementos cortafuegos, uno para aislar dicha zona de la red interna y otro para aislarla de la externa, preferiblemente de tecnologías diferentes para evitar que un problema de seguridad concreto en uno de ellos repercuta en el otro y por tanto en toda la organización. Esta arquitectura suele aportar un nivel de seguridad elevado, pero por el contrario también tiene un sobrecoste para la organización. La segunda aproximación para la definición de una DMZ se basa en el uso de un único elemento cortafuegos (redundado o no) para separar zonas de red (interna/DMZ/Internet), mediante el uso de tarjetería de red adicional en el sistema (se requiere al menos una tarjeta por cada zona de la red). Esta aproximación ofrece un nivel de seguridad a priori menor que la anterior, pero por el contrario los costes de implantación y mantenimiento suelen ser menores, por lo que es la más utilizada. Como se ha indicado con anterioridad, cada organización debe evaluar qué solución es la más adecuada en su caso concreto; en la mayoría de situaciones, un único sistema cortafuegos correctamente configurado y con diferentes interfaces de red es aceptable desde el punto de vista de seguridad ([mp.com.1]), pero en el caso de categoría ALTA, el ENS especifica como obligatoria la utilización de dos o más equipos de diferente fabricante en cascada y con sistemas redundantes que garanticen la continuidad en caso de fallo técnico.

68. En cualquier caso, el cortafuegos o los cortafuegos corporativos deberán controlar el tráfico que se permite hacia los sistemas de correo, tanto desde los equipos internos a la organización como desde los equipos ubicados en Internet; en una arquitectura estándar, se requerirá acceso desde Internet al servicio SMTP del servidor (para poder recibir correo electrónico externo a la organización), así como acceso a través del mismo protocolo desde dicho servidor a Internet (para poder enviar correo electrónico a direcciones externas a la organización). Desde la red interna, además de acceso SMTP al servidor (no al contrario), es habitual que se requiera acceso POP e IMAP, así como sus equivalentes seguros, para que los usuarios puedan descargar el correo desde el servidor hacia sus equipos.

69. Adicionalmente a las reglas anteriores, es importante que la organización evalúe la conveniencia de denegar, en el cortafuegos corporativo, todo el tráfico SMTP saliente

hacia Internet con excepción del generado en los servidores de correo electrónico; esto evitará, entre otros, propagaciones masivas de malware desde equipos de usuario, uso de equipos internos para realizar ataques de phishing, etc. Como inconveniente, los usuarios que utilicen diferentes servidores de correo –por ejemplo, que gestionen diferentes cuentas desde su equipo-, no podrán hacerlo salvo que, una a una, se permitan estas conexiones SMTP salientes en el cortafuegos de la organización.

70. Se muestra gráficamente una arquitectura de red tipo para la definición de un sistema de correo seguro:



71. Al menos en los entornos de categoría ALTA la organización debe implantar en la arquitectura sistemas de detección o prevención de intrusiones basados en red (NIDS/NIPS) que permitan identificar o incluso detener ataques o tráficos anómalos contra la plataforma de correo corporativo ([op.mon.1]); los registros generados por estos entornos deben ser correctamente analizados, como cualesquiera registros de auditoría, para garantizar que se emprenden las acciones adecuadas ante una posible violación de la seguridad.

2.2. BASTIONADO DEL SISTEMA

72. De la misma forma que el resto de sistemas corporativos, es crítico que los servidores de correo estén correctamente bastionados a nivel de sistema operativo. Para ello, debemos seguir las guías STIC correspondientes a nuestro sistema concreto y aplicar en éste las directrices que marcan dichos documentos.

73. El servidor o servidores de correo corporativo deben estar en sistemas dedicados, no compartiendo su funcionalidad con otros entornos de la organización para evitar que vulnerabilidades en éstos afecten al correo electrónico. El software instalado en el servidor debe ser mínimo, eliminado aplicaciones no estrictamente necesarias para el

funcionamiento del sistema de correo (herramientas ofimáticas, entornos de desarrollo, etc.) y, por supuesto, deben considerarse siempre las directrices de bastionado contempladas en las guías STIC de aplicación en cada entorno.

74. En términos generales, debemos considerar siempre los siguientes extremos:

75. Aplicación de parches y actualizaciones de seguridad en el sistema tan pronto como sea posible.

76. Eliminación de los servicios no necesarios para el funcionamiento correcto del sistema.

77. Restricciones de acceso adecuadas, tanto desde la red interna como desde Internet.

78. Políticas de gestión de usuarios y contraseñas robustas.

79. Permisos correctos en todo el sistema de archivos, pero prestando especial atención a las carpetas de correo de los usuarios.

80. Monitorización y control de parámetros que impliquen anomalías en la seguridad.

81. Se detalla a continuación cada uno de los aspectos anteriores.

2.2.1. PARCHES Y ACTUALIZACIONES

82. Los servidores de correo corporativos deben estar incluidos en la política de actualizaciones de seguridad de la organización, denominada habitualmente P&V (Parches y Vulnerabilidades). Esta política debe definir el ciclo de análisis y parcheo de sistemas, y debe aplicarse tanto al sistema operativo como a las aplicaciones relevantes en la gestión del correo electrónico, contemplando los siguientes aspectos sin menoscabo de otros cualesquiera que la organización considere:

83. Inventario. La organización debe disponer de un inventario de elementos intervinientes en la gestión del correo electrónico, incluyendo versiones de sistemas operativos y aplicaciones, configuraciones relevantes en cuanto a seguridad, niveles de parcheado, etc. Esta información será la base del análisis de qué vulnerabilidades afectan o pueden afectar a la seguridad del correo electrónico, y por tanto debe ser actualizada de forma permanente.

84. Obtención de información. Análisis y monitorización de fuentes de información relativas a P&V. Es obligatorio en cualquier caso recibir información de seguridad del propio fabricante o proveedor del sistema, generalmente a través de listas de correo específicas o de soporte directo; de forma adicional, es importante que la organización evalúe la conveniencia de monitorizar otras fuentes significativas que puedan proporcionar información relativas a problemas de seguridad lógica sobre el entorno: listas de correo, foros, blogs…

85. Análisis. Ante la recepción de información relevante para la seguridad del entorno de correo electrónico, la organización debe evaluar el riesgo asociado a cada situación y la conveniencia de aplicar parches o actualizaciones en los diferentes entornos afectados. Dicho análisis debe ser realizado de forma conjunta por parte del personal de seguridad y por parte del personal técnico responsable de la administración de la plataforma.

86. Obtención de parches. Si del análisis anterior se deriva la necesidad de aplicar parches o actualizaciones sobre la plataforma de correo, los mismos deben ser facilitados por el proveedor correspondiente a través de los canales habilitados a tal efecto en cada organización (repositorios software, listas de correo…).

87. Aplicación de parches. Una vez obtenidos los parches o actualizaciones deben ser aplicados en los sistemas y aplicaciones correspondientes. Para ello el equipo administrador de la plataforma debe realizar las pruebas necesarias en entornos fuera del ámbito de producción (habitualmente llamados de test o preproducción) antes de la aplicación efectiva, y una vez verificado el correcto funcionamiento en estos entornos, aplicarlos en el entorno real en horario de mínimo impacto y con las precauciones correspondientes (procedimientos de restauración, marcha atrás, etc.) definidas en los procedimientos corporativos.

88. Verificación. Una vez aplicados satisfactoriamente los parches o actualizaciones correspondientes, el equipo de seguridad debe verificar, preferiblemente con pruebas técnicas, que dicha aplicación corrige la vulnerabilidad o vulnerabilidades que motivaron cada actualización, confirmando así que el riesgo ha sido mitigado.

89. El procedimiento P&V corporativo debe ser aplicado al menos una vez al mes en condiciones normales, y de forma extraordinaria siempre que se determine la presencia o presencia potencial de vulnerabilidades significativas en el entorno de correo electrónico que puedan introducir riesgos para la información corporativa.

2.2.2. ELIMINACIÓN DE SERVICIOS

90. Como en el resto de sistemas de la organización, en los servidores que proporcionan el correo electrónico corporativo, debemos eliminar los servicios que no sean estrictamente necesarios para el correcto funcionamiento de la plataforma; esto implica, teniendo en cuenta que el servidor de correo debe ser un sistema dedicado, la eliminación de todos los servicios de red ajenos al correo electrónico.

91. En función del sistema operativo utilizado como plataforma de correo, podremos deshabilitar los servicios no necesarios de una u otra forma, bien mediante utilidades proporcionadas a tal efecto por el sistema operativo (Windows, AIX, Solaris 10…) bien mediante la simple modificación de archivos y la posterior aplicación de dicha configuración (Linux, Solaris 9, FreeBSD…). En cualquier caso, es habitual la deshabilitación en la plataforma servidora de correo de, entre otros, los siguientes servicios (sin menoscabo de otros cualesquiera en función de cada caso):

92. Servicios de impresión de documentos (CUPS, LPD…).

93. Servicios de compartición de ficheros (NFS, SMB…).

94. Servidores web o de aplicaciones (Apache, IIS, Tomcat…), con excepción de los usados para *webmail*.

95. Servicios simples TCP (chargen, echo, daytime…).

96. Servicios de gestión remota con excepción de los estrictamente necesarios para la administración del sistema (SSH, VNC, Terminal Remota…).

97. Deshabilitar los servicios innecesarios es crítico en cualquier proceso de bastionado, pero en los entornos que proporcionan correo electrónico, debido a la sensibilidad de la información que pueden manejar, es más importante si cabe. Un servicio abierto en el servidor que no interviene en la gestión del correo electrónico es una potencial puerta de acceso al sistema, introduce riesgos innecesarios para la organización y puede llegar a dificultar incluso la detección de problemas de seguridad, con lo que debe ser eliminado.

98. Tanto en Unix como en Windows podemos ver los servicios de red que están escuchando en un puerto de nuestro sistema mediante la orden netstat, con las opciones correspondientes.

2.2.3. CONTROL DE ACCESOS

99. Tal y como se ha indicado con anterioridad, el servidor de correo corporativo debe estar instalado en una zona desmilitarizada de la red, DMZ, y debemos controlar adecuadamente el tráfico entre dicho servidor y otras zonas de red, incluyendo Internet, mediante uno o más elementos cortafuegos.

100. Hemos indicado previamente los flujos de tráfico que deben estar permitidos en el cortafuegos en relación al servicio de correo; en resumen, y siempre en términos generales –cada organización debe evaluar sus requisitos y necesidades y adaptar la presente guía a los mismos ([op.acc.2])-, deberemos garantizar que el cortafuegos:

101. Permite tráfico SMTP desde Internet hacia el servidor.

102. Permite tráfico SMTP/POP3/IMAP o equivalentes desde la red interna hacia el servidor.

103. Permite tráfico SMTP saliente desde el servidor hacia Internet.

104. Bloquea tráfico SMTP saliente desde equipos que no sean el servidor corporativo hacia Internet.

105. Permite tráfico administrativo (gestión del servidor vía SSH, Terminal Remota…) desde los puestos del personal correspondiente de la red interna hacia el servidor, bloqueando el resto.

106. Bloquea por defecto todo el tráfico entre redes no permitido expresamente.

107. Adicionalmente a las restricciones de acceso a nivel de red indicadas con anterioridad, la mayor parte de sistemas operativos y servidores de correo permiten especificar, a nivel de aplicación, desde qué orígenes (IP) es permitido el acceso al equipo, tanto a nivel de administración como a nivel de utilización. Es necesario que cada organización analice esta posibilidad que ofrecen los servidores y se implanten las restricciones a este nivel necesarias para garantizar que sólo el personal técnico autorizado puede acceder al sistema para administrarlo y sólo el personal de la organización, desde las direcciones IP permitidas, pueden acceder al servicio de correo para la gestión de sus buzones.

2.2.4. AUTENTICACIÓN

108. Dentro del proceso de bastionado y refuerzo de la seguridad del servidor de correo, es necesario eliminar todos los usuarios del entorno, tanto a nivel de aplicación como de sistema, que no sean estrictamente necesarios para el correcto funcionamiento del correo corporativo. El acceso para gestión del servidor debe estar limitado a unos pocos usuarios de las áreas técnicas correspondientes, siempre con usuarios nominales y registrando hasta donde técnicamente sea posible las acciones ejecutadas en dichos accesos. Esta restricción debe considerarse especialmente en aquellos usuarios generados por defecto en el sistema o en la aplicación, ya que en ocasiones sus contraseñas son conocidas o ni siquiera solicitan una clave para iniciar una sesión interactiva.

109. Es habitual que existan en el servidor de correo cuentas de sistema o aplicación que no pueden ser eliminadas, pero que no requieren de un inicio de sesión interactivo: se trata

de cuentas necesarias para el funcionamiento de la plataforma pero que no corresponden a usuarios que conecten al sistema para lanzar órdenes. En estos casos, a tales usuarios se les debe restringir la capacidad de inicio de sesión interactiva para evitar que puedan ser utilizados por un atacante, por ejemplo mediante el empleo de *shells* como */bin/false* en entornos Unix.

110. Las políticas de contraseñas corporativas deben aplicarse obviamente sobre el sistema de correo, tanto a nivel de sistema operativo como a nivel de aplicación. Estas políticas deben ser capaces de generar contraseñas suficientemente robustas (longitudes mínimas, uso de mayúsculas, minúsculas y caracteres alfanuméricos, tiempos de vida máximos y mínimos...) para los usuarios y administradores del sistema, incluyendo a los usuarios exclusivos del correo –probablemente todo el personal de la organización-, de forma que se dificulte la adivinación de claves por parte de un atacante.

111. Muchas organizaciones incluyen en las políticas de autenticación de usuarios bloqueos de cuenta tras superar un número determinado de intentos de acceso inválidos. Las organizaciones deben evaluar cuidadosamente este control, ya que cualquier atacante puede causar de forma trivial una negación de servicio (DoS) sobre el entorno de correo corporativo, evitando que usuarios autorizados puedan gestionar legítimamente su e-mail; en caso de aplicación de esta salvaguarda, no debemos permitir el bloqueo del usuario de administración de la plataforma, ya que podríamos encontrarnos ante problemas de disponibilidad relativamente graves. Es preferible, y la organización debe analizar la conveniencia de esta medida, no bloquear el acceso tras superar un número máximo de intentos de conexión, sino monitorizar en tiempo real esta situación y, en caso de producirse, notificar inmediatamente al área de seguridad corporativa para que aplique las medidas correspondientes en cada caso.

2.2.5. PERMISOS

112. Cualquier sistema operativo de propósito general proporciona un control de acceso a los objetos (ficheros) suficientemente granular para la mayor parte de organizaciones, basado en un modelo DAC (Control de Accesos Discreccional) que permite determinar quién y cómo accede a los diferentes archivos, directorios y recursos en general del sistema. Los administradores del sistema deben garantizar que únicamente los usuarios autorizados acceden a sus buzones de correo en el servidor y que los permisos de dichos buzones –archivos generalmente, a nivel de sistema operativo- son adecuados y evitan que usuarios sin privilegios puedan acceder al correo de personas en el servidor.

113. No obstante, esta aproximación tiene un inconveniente, y es que los usuarios privilegiados del sistema (root, administrador…) pueden, en muchos entornos, acceder al contenido de estos buzones de una u otra forma. Algunos entornos de correo introducen buzones cifrados que no pueden ser accedidos más que por el propietario de los mismos, por lo que las organizaciones deben evaluar la conveniencia de aplicar este control si técnicamente es factible, analizando las connotaciones legales correspondientes (trazabilidad e interceptación justificada).

114. En cualquier caso, el acceso privilegiado al entorno de correo debe permanecer restringido a unas pocas personas del área técnica correspondiente y las acciones de dichos accesos deben ser convenientemente trazadas para detectar cualquier situación anómala, en especial aquellas que puedan implicar pérdidas de confidencialidad. En este sentido, los aspectos relativos a segregación de tareas son críticos en cualquier entorno,

pero lo suelen ser más aún en los que gestionan el correo corporativo de la organización, por lo que los accesos y las acciones ejecutadas por los administradores de la plataforma de correo deben ser revisadas por el personal del área de seguridad corporativa con una periodicidad al menos mensual; esta salvaguarda debe considerarse obligatoria en entornos de nivel medio o alto ([op.acc.3]).

2.2.6. MONITORIZACIÓN Y CONTROL

115. Los servidores que gestionan el correo electrónico corporativo deben ser objeto de una especial monitorización que garantice el control de las actividades desarrolladas en los mismos y permita a la organización actuar rápidamente ante potenciales violaciones de su seguridad. En el apartado correspondiente a registros y auditoría de la presente guía se muestran algunos de los elementos que es necesario monitorizar a partir de los registros del sistema, de forma que una situación anómala sea detectada y procesada en el menor tiempo posible desde que se produce.

116. Una medida de seguridad adicional al análisis de registros que en ocasiones puede ser útil para detectar violaciones de la seguridad, y que por tanto cada organización debe analizar la conveniencia de su implantación, es la monitorización de acceso a determinados buzones de correo críticos; para ello, muchos sistemas operativos proporcionan registro de acceso a ficheros, indicando quién accedió a un determinado objeto, cuándo y de qué forma lo hizo. Esta información debe ser procesada independientemente del área técnica que gestione el servidor y remitida en exclusiva al área de seguridad corporativa para su análisis posterior.

117. Otra salvaguarda que la organización debe evaluar es la utilización de señuelos o *honeytokens*, en este caso buzones ficticios de usuarios inexistentes que generarán una alerta al área de seguridad siempre que sean accedidos –quizás con excepción de los sistemas de copia de la organización-, permitiendo así la detección temprana de barridos de los buzones –incluso a nivel de sistema operativo- y evitando posibles robos de información. Esta salvaguarda se enmarca en las medidas de seguridad del marco operacional, concretamente [op.mon.1], detección de intrusos.

2.3. SEGURIDAD DE LOS SERVICIOS DE CORREO

118. Además del bastionado habitual a nivel de sistema operativo, los servicios asociados al correo electrónico deben también configurarse de manera segura. Es especialmente importante garantizar, en primer lugar, que las versiones de las diferentes aplicaciones utilizadas para la gestión del correo en el servidor sean correctas tanto desde el punto de vista funcional como desde el punto de vista de seguridad, aplicando las actualizaciones proporcionadas por el fabricante siempre que sea necesario. En segundo lugar, es necesario garantizar que la configuración de estas aplicaciones es correcta también desde ambos puntos de vista, ya que aplicaciones actualizadas convenientemente pero con una deficiente configuración son susceptibles de ser atacadas con éxito por un tercero (típicamente, para utilizar el servidor como *relay* en el envío de SPAM).

119. Se debe restringir el acceso a los servicios de acceso al correo electrónico a aquellos orígenes desde los que efectivamente sea necesario acceder a la gestión de los mensajes por parte de los usuarios. La organización debe evaluar muy cuidadosamente los riesgos asociados a permitir el acceso a los servicios de correo desde toda Internet, algo muy habitual debido a requisitos de movilidad o simplemente a funcionalidad para los

usuarios pero que introduce un **riesgo muy considerable** en la mayor parte de situaciones, ya que suele ir asociado al uso de equipos ajenos a la organización y a sus políticas de seguridad, equipos por tanto no controlados adecuadamente y que pueden ser un potencial punto de fuga de información: si un usuario utiliza un equipo comprometido para acceder a su correo electrónico no sólo se podrá interceptar dicho correo, sino también credenciales de acceso, claves de cifra, etc.

120. En caso de que sea necesario el acceso a servicios de envío de correo desde Internet, es necesario garantizar en el tiempo que el servidor de correo no actúa como *open relay*, es decir, no permite ser utilizado para el envío de correo no deseado. Si esta situación se produce, aparte del problema de seguridad asociado y del impacto directo en la organización, es posible que el servidor corporativo sea incorporado a una lista negra y por tanto bloqueado automáticamente en múltiples MTA, con el riesgo reputacional que esto implica y el problema operativo que se puede llegar a producir al no poder enviar correos a través de los MTA que nos bloquean.

121. Una aproximación común en la protección de servicios de correo utilizados desde Internet, sin menoscabo de otras cualesquiera, es una estrategia *POP before SMTP*, que de forma transparente al usuario le obliga a autenticarse mediante POP3 antes de poder enviar un correo desde el servidor (protocolo SMTP) desde cualquier punto de la red durante un intervalo de tiempo determinado.

122. En el caso particular en que se requiera acceso web al correo corporativo, la organización debe garantizar la imposibilidad de acceder al entorno evitando la autenticación de éste ([mp.s.2]); de la misma forma, la organización debe garantizar que los ataques vía web más habituales (XSS, SQL-i, LFI, RFI…) no afectan a la seguridad del servicio o aplicación web, bien mediante la implantación de sistemas de prevención de intrusiones que detecten y detengan los ataques antes de llegar al servidor, bien mediante un correcto bastionado del entorno web que proporciona correo electrónico a la organización.

123. En cualquier caso, la organización debe evaluar los riesgos asociados a permitir los accesos web al correo corporativo desde toda Internet, de la misma forma que debe hacerlo a la hora de habilitar cualquier protocolo de acceso al correo electrónico o a la infraestructura tecnológica en general; es necesario recordar que el hecho de facilitar a los usuarios gestión web de su correo no tiene por qué implicar que éstos puedan conectar al mismo desde cualquier ubicación.

124. Independientemente de desde dónde esté permitido el acceso vía web al correo, el servidor web no debe estar ubicado en el propio MTA corporativo, sino en un servidor independiente a éste, y por supuesto su bastionado y auditoría debe ser correcto y completo en el tiempo. Todas la comunicaciones entre el navegador –cliente- y el servidor web deben estar obligatoriamente cifradas, incluyendo en primer lugar la autenticación de usuarios; las comunicaciones mediante protocolo HTTP sin soporte SSL/TLS no son aceptables en ningún caso. Adicionalmente, el servidor web debe proporcionar mecanismos de terminación automática de la sesión web tras un periodo de inactividad, y éstos deben estar correctamente implantados en la organización, de acuerdo a las políticas de seguridad corporativas, para evitar la reutilización de sesiones y por tanto posibles fugas de información.

Nota: el soporte SSL/TLS del servidor web debe ser aceptable desde el punto de vista de seguridad corporativa, tanto en lo referente a la longitud de claves (mínimo 128 bits) como en lo referente a las versiones de protocolos (mínimo v3 en el caso de SSL).

2.4. ADMINISTRACIÓN DEL SERVIDOR

125. Como se ha indicado, los servidores de correo son un elemento a proteger especialmente, ya que se encargan de gestionar (envío, recepción, almacenamiento…) los mensajes de correo electrónico de toda una organización o de buena parte de ella. Por este motivo, son objeto habitual de ataques, ya que si un tercero obtiene acceso a estos sistemas, podrá utilizarlos, entre otros ataques, para escuchar la información en tránsito o almacenada en los mismos.

126. La administración de los entornos de correo debe basarse obligatoriamente en procedimientos documentados y aprobados por la organización ([org.3]), que detallen cómo llevar a cabo las tareas habituales de administración (generación de nuevas cuentas de correo, restauración de contraseñas…), quién debe ejecutar dichas tareas y quién debe aprobarlas y validarlas. Adicionalmente, como en cualesquiera procedimientos documentados de la organización, deben establecerse los mecanismos para identificar y reportar comportamientos anómalos, tal y como detalla el punto correspondiente a registros y auditoría del sistema en la presente guía.

127. Como en otros entornos tecnológicos de la organización, es importante que en los sistemas de correo existan dos grupos de administradores: los administradores del sistema (entendiendo por sistema tanto el operativo como sus aplicaciones), a los que les corresponde la explotación del entorno y la garantía de que el funcionamiento es correcto, y los administradores de seguridad, que tienen por objeto garantizar que el sistema es seguro desde todos sus puntos de vista (lógico, operacional, físico, etc.). Las funciones y responsabilidades de ambos equipos de trabajo deben estar claramente segregadas ([op.acc.3]).

128. La administración del servidor de correo, como del resto de elementos tecnológicos de la organización, suele realizarse de forma remota; los administradores del sistema conectan al servidor, habitualmente desde sus equipos de usuario de la organización, mediante protocolos como SSH (Unix) o Terminal Remota (Windows). Para la mayor parte de organizaciones no es viable la administración en local (es decir, con el operador o administrador del sistema sentado directamente frente a su consola) ni del correo electrónico ni de otros servicios corporativos, por lo que al permitir que usuarios privilegiados conecten a través de la red al servidor se introducen riesgos que es necesario minimizar en cualquier entorno y con independencia del nivel en que se clasifique al sistema de correo electrónico. Es obligatorio, en todos los casos, seguir las siguientes directrices para la administración remota del servidor:

129. Uso de protocolos cifrados para la conexión remota.

130. Restricción por IP de los sistemas desde donde se puede iniciar sesión de administración en el servidor de correo. Únicamente se deben permitir dichas conexiones desde redes internas a la organización, en ningún caso desde Internet salvo en el caso de conexión a través de redes privadas virtuales correctamente configuradas y monitorizadas.

131. Uso de mecanismos de autenticación robusta (típicamente, certificado con contraseña).

132. Uso de usuarios nominales que ejecuten tareas con privilegios estrictamente cuando es necesario y dejando traza de dicha ejecución. Todos los usuarios por defecto o que no requieran acceso remoto para administrar el sistema deben ser eliminados.

2.4.1. COPIAS DE RESPALDO

133. Las tareas relativas a copias de respaldo y restauración son habitualmente un punto clave en la administración de cualquier entorno tecnológico ([mp.info.9]); en el caso de los servidores de correo, dado su carácter vital para la organización, estas tareas son por supuesto críticas para garantizar que podemos recuperar el sistema hasta un punto determinado por la política de seguridad corporativa. Es obligatorio que la organización defina, aplique y audite una política de copias de respaldo y restauración general abarcando a todos los sistemas relevantes para el servicio, en particular a los servidores que hospedan el correo corporativo. Dicha política debe contemplar los requisitos de seguridad de la organización –clasificación y tratamiento de la información, tiempos de restauración…- pero también cualesquiera requerimientos legales, contractuales o normativos que sean de aplicación, en especial los relativos a la protección de datos de carácter personal y al mantenimiento de registros significativos.

134. Como se ha indicado, la política de copias de respaldo de la organización debe cubrir adecuadamente las necesidades corporativas de seguridad contemplando, en el caso particular de los servidores de correo, copias periódicas de la configuración del sistema y de las aplicaciones que proporcionan el servicio de correo electrónico. De la misma forma, debe cubrir la copia de los buzones de correo almacenados en el servidor con una frecuencia diaria, mitigando así los problemas de pérdidas de información en el caso de un desastre. La organización debe seleccionar un entorno de correo que soporte la ejecución de copias en caliente, sin necesidad de detener el sistema, ya que por la criticidad habitual de estos entornos no es posible detenerlos para ejecutar la copia. Esto es especialmente relevante en los sistemas que almacenan los buzones con un formato propietario o de base de datos, ya que en ocasiones el proceso estándar de copia puede no servir para respaldar correctamente lo mismos.

Nota: muchas herramientas de backup soportan la copia en caliente de entornos de correo, bien de forma directa bien mediante software adicional a la herramienta. Es necesario confirmar que nuestra herramienta de copias es capaz de respaldar adecuadamente la información ubicada en los buzones personales de los usuarios.

135. Para confirmar que las copias son correctas y completas, la organización debe definir una política de restauraciones periódicas de la información, de forma que se puedan detectar problemas en el proceso de copia antes de que tengan impacto sobre el negocio. Estas pruebas periódicas de restauración deben contemplar diferentes escenarios, marcados en cada caso por las necesidades corporativas, pero que comprendan al menos los siguientes supuestos:

136. Restauración completa del sistema ante un problema grave.

137. Restauración del servicio de correo electrónico ante problemas en las aplicaciones que lo prestan.

138. Restauración de buzones de usuarios ante problemas particulares o errores de operación, como borrados accidentales.

139. En cada caso deberá definirse la periodicidad correspondiente a las pruebas asociadas a cada situación; para el caso de buzones de usuario, la organización debe fijar al menos unas pruebas de restauración mensuales, con independencia de las solicitudes de restauración reales que estos usuarios soliciten al departamento técnico correspondiente.

140. Adicionalmente, es necesario considerar, dentro de la política de copia y restauración corporativa, que los buzones de usuario pueden contener información muy sensible de la organización, por lo que las personas responsables de ejecutar y verificar las restauraciones de los mismos deben estar debidamente acreditadas para la gestión de la información correspondiente en cada caso. Si los buzones de usuario están cifrados mediante contraseña propia de cada usuario, la verificación de una restauración deberá contar obligatoriamente con la participación de dicho usuario para introducir la clave, que obviamente no podrá ser facilitada a otras áreas de la organización.

141. Las copias de respaldo deben estar sujetas a las mismas restricciones de seguridad que los sistemas que contienen la información, y deben clasificarse en función de la clasificación más alta de la información que puedan ser susceptibles de contener. De esta forma, los medios donde se ubiquen las copias requerirán de niveles de seguridad aceptables en cualquier caso, incluyendo salvaguardas de seguridad física y medioambiental ([mp.si.3]), lógica, organizativa y legal. Todos estos medios deben estar etiquetados convenientemente sea cual sea el nivel definido para el sistema ([mp.si.1]), de forma que sin revelar su contenido se indique el nivel de seguridad de la información que contienen y los usuarios de estos medios puedan interpretar el significado del etiquetado. Aproximaciones habituales son los códigos de barras para los medios de almacenamiento secundario o el simple uso de códigos alfanuméricos internos a la organización que puedan ser modificados periódicamente, garantizando así que personal que cesa en sus funciones o abandona la organización no sea capaz de interpretar con posterioridad el contenido de un medio a partir de su etiquetado.

142. La custodia de los medios de copia de respaldo, independientemente del nivel de la información que contienen, debe realizarse garantizando el correcto control de acceso físico a dichos medios (ubicación en áreas separadas y con acceso restringido a las mismas, [mp.if.1] y registros de entrada o salida de medios, [mp.if.7]) y unos parámetros medioambientales de conservación acordes a las especificaciones del fabricante en cada caso ([mp.si.3]).

143. En el caso de copias de respaldo de sistemas de nivel medio o alto es obligatorio el cifrado del medio donde se ubica la copia ([mp.si.2]) si se trata de elementos móviles (habitualmente, cintas de backup) o susceptibles de abandonar las premisas de la organización y por tanto sus medidas de protección. En este caso, si se realiza un transporte de medios, con independencia del nivel del sistema o sistemas respaldados deben contemplarse las salvaguardas definidas en [mp.si.4]:

144. Registro de salida que identifique al transportista que recibe un soporte para su traslado.

145. Registro de entrada que identifique al transportista que entrega un soporte.

146. Procedimiento rutinario de cotejo de salidas y llegadas de soportes, generando alerta ante posibles incidentes.

147. Protección criptográfica correspondiente al nivel más alto de la información contenida en el medio.

148. Protección de claves de cifrado ([op.exp.11]) durante su ciclo de vida completo, en función del nivel de la información almacenada.

2.4.2. GESTIÓN DE USUARIOS

149. La identificación de usuarios para acceder al entorno de correo –como en el resto de infraestructura corporativa- debe realizarse en base a un procedimiento formalmente definido en la organización ([op.acc.1]) que contemple la identificación unívoca de cada usuario y los modelos de gestión aplicables, en especial los asociados a la revocación de cuentas de acceso y periodos de retención, según las directrices definidas en el ENS con independencia del nivel de cada sistema. De la misma forma, deben adecuarse los mecanismos de autenticación en el entorno de correo electrónico en función de la categoría del sistema ([op.acc.5]); en concreto, la autenticación mediante contraseña en exclusiva está especialmente prohibida en sistemas de nivel ALTO. En el anexo correspondiente de la presente guía se aporta un modelo tipo de normativa de identificación y autenticación para que las organizaciones puedan adaptarlo según sus requisitos y necesidades de seguridad.

150. Los derechos de acceso de cada usuario al entorno de correo electrónico deben limitarse atendiendo a los criterios de mínimo privilegio, necesidad de conocer y capacidad de autorizar, con independencia del nivel en el que se incluya a los sistemas en cada caso ([op.acc.4]). Habitualmente los entornos de correo no dispondrán de la granularidad suficiente para establecer niveles de acceso a nivel de aplicación, por lo que las organizaciones deben analizar la necesidad de establecer controles compensatorios con independencia de la aplicación de correo corporativa. Adicionalmente, la organización debe definir con claridad quién posee la capacidad de conceder, alterar o anular la autorización de acceso al correo electrónico y de qué forma debe hacerlo, garantizando que este proceso sea lo suficientemente ágil como para no introducir riesgos innecesarios en la organización (típicamente, accesos que deben ser revocados y que por motivos técnicos u organizativos no lo son).

151. La organización debe implantar una política de revisiones periódicas de usuarios en el servidor de correo –extensible por supuesto al resto de entornos corporativos- de forma que al menos mensualmente se validen los usuarios personales con acceso al servidor, los usuarios propios del sistema y de la aplicación de correo y, en especial, los usuarios con privilegios tanto a nivel de operativo como de aplicativo. Dicha revisión periódica debe permitir bloquear o eliminar aquellos usuarios no considerados necesarios para el correcto funcionamiento del entorno, como aquellos que han superado un umbral de inactividad, aquellos que han abandonado la organización, etc., de forma independiente a cualesquiera otros procedimientos que puedan permitir evitar o detectar estas situaciones: gestión de bajas de usuario, controles técnicos, etc.

2.4.3. CONTINUIDAD DEL SERVICIO

152. Dada la criticidad de los servicios de correo electrónico en cualquier organización es muy importante garantizar, en todos los casos, que dichos servicios podrán ser recuperados de forma satisfactoria ante un desastre, en un tiempo acotado y aceptado por la Dirección. Para ello, en los sistemas de nivel medio o alto, la organización debe realizar un análisis

de impacto (BIA, *Business Impact Analysis*) que permita determinar los requisitos de disponibilidad del servicio de correo electrónico (en función del impacto de una interrupción durante un cierto periodo de tiempo) e identificar qué sistemas son críticos para la prestación de dicho servicio ([op.cont.1]).

153. El análisis de impacto a realizar en los casos en los que sea de aplicación marcará el tiempo de recuperación objetivo (RTO, *Recovery Time Objective*) del servicio de correo electrónico, entendido como el tiempo en el que es necesario restaurar dicho servicio para que las consecuencias para la organización no sean graves. Dada la criticidad habitual del correo electrónico, la organización debe evaluar el orden de magnitud del RTO en función del nivel en el que se clasifica este servicio; se presentan, a modo de ejemplo, RTO para los niveles medio y alto (los únicos de aplicación de la salvaguarda en base al ENS):

NIVEL	Tiempo de recuperación objetivo (h)
ALTO	RTO < 4
MEDIO	RTO < 12

154. Adicionalmente a los requisitos de disponibilidad anteriores, el BIA debe identificar qué sistemas son críticos para la prestación del servicio de correo electrónico; podemos entender el servicio como una pirámide de necesidades, en la que el propio servicio es la cúspide de dicha pirámide. Por debajo del **servicio** se requerirán que estén operativas una serie de aplicaciones necesarias para el correcto funcionamiento del mismo (la aplicación de transporte de correo es el principal ejemplo, pero también pueden serlo servicios web o elementos de autenticación adicionales que sean requeridos para garantizar que el servicio es correcto), y por debajo de éstas una serie de **software base** (bases de datos, servicios web, servicios LDAP… por citar unos ejemplos) que es a su vez necesario para que las aplicaciones funcionen adecuadamente. Por último, en la base de la pirámide definida con anterioridad encontraremos la **infraestructura** necesaria (electrónica de red, servidores, cortafuegos…) para que todos los niveles superiores funcionen correctamente.

155. Obviamente, la organización debe garantizar que, ante un desastre, es capaz de recuperar todos los elementos implicados en la prestación del servicio de correo electrónico en los RTO correspondientes; para ello, y de obligatorio cumplimiento en los entornos de nivel alto, debe desarrollarse un plan de continuidad ([op.cont.2]) que defina las acciones a ejecutar en caso de interrupción del servicio de correo, contemplando los aspectos indicados en el ENS e integrado con el resto de planes de continuidad –o un plan de continuidad global- de la organización. Dicho plan debe ser probado al menos anualmente ([op.cont.3]) mediante un ejercicio de simulacro que permita a la organización identificar y corregir errores en el plan de continuidad, mejorando así el mismo en el tiempo.

2.5. REGISTROS Y AUDITORÍA DEL SISTEMA

156. Todos los entornos de correo generan registros de auditoría, tanto a nivel de sistema operativo como a nivel de aplicación o de base de datos; desde el punto de vista de seguridad, nos interesan aquellos registros relevantes para garantizar la integridad, confidencialidad y disponibilidad de los sistemas y, especialmente, de la información que procesan. A la hora de implantar un entorno de correo corporativo, es necesario que la

organización evalúe no sólo sus requisitos de funcionalidad, sino también los requisitos de seguridad (disponibilidad de actualizaciones, histórico de vulnerabilidades relevantes, integración con herramientas de monitorización de la seguridad…) y dentro de ellos, preste especial atención a las capacidades de registro de entorno, tanto a nivel de sistema operativo como de aplicación (conexiones de red y gestión de mensajes). En el caso de sistemas de nivel medio o alto el registro es obligatorio para las actividades de los usuarios, en los términos definidos en el ENS ([op.exp.8]) en cada caso.

157. Los registros de actividad del sistema, de la aplicación o de los usuarios deben protegerse convenientemente en cualquier caso, pero para sistemas de nivel alto dicha protección es obligatoria en los términos definidos en el ENS ([op.exp.10]), garantizando que los registros no puedan ser modificados ni eliminados de forma no controlada y que las copias de los mismos estarán sujetas a niveles de protección equivalentes a los de los propios registros y que el periodo de retención está formalmente definido en la organización. Adicionalmente se aplicarán marcas de tiempo según [mp.info.5], y en todos los casos los registros de diferentes sistemas deben estar sincronizados en fecha y hora, por ejemplo mediante el uso de un servidor de tiempos NTP centralizado en la organización.

158. Con estas premisas, es necesario que los registros de auditoría del sistema sean procesados convenientemente en busca de anomalías o entradas que puedan suponer una potencial violación de la seguridad del sistema. Algunos ejemplos de elementos a revisar, sin menoscabo de otros cualesquiera, son los siguientes:

159. Intentos de accesos fallidos al sistema o aplicaciones de correo por parte de usuarios privilegiados.

160. Conexiones al sistema o aplicaciones de correo fuera de horario por parte de usuarios privilegiados.

161. Número excesivo de conexiones legítimas al sistema fuera del horario habitual de trabajo.

162. Indicios de actividad excesiva en horario no laboral (consumo de CPU, E/S, memoria…).

163. Accesos simultáneos o cercanos en el tiempo con diferentes nombres de usuario desde un mismo origen.

164. Número elevado de intentos de acceso fallido y posteriormente accesos legítimos desde un mismo origen.

165. Esta revisión debe realizarse con una periodicidad adecuada y acorde a los requisitos de seguridad de cada organización, desde varias veces al día hasta una vez al mes; revisiones con periodicidades superiores no deben ser admitidas corporativamente. Adicionalmente, la organización debe evaluar la necesidad de automatizar dichas revisiones, integrando los registros del sistema con elementos de correlación y gestión de alertas que sean capaces de notificar en tiempo real la presencia de entradas anómalas en los entornos de correo. Esto es debido a que el proceso de revisión, en caso de revisarse de forma manual, presenta dos grandes problemas: la probabilidad de fallo humano (es posible ignorar en la revisión entradas relevantes para la seguridad) y los recursos utilizados en la revisión: se trata de un proceso relativamente costoso que, en caso de repetirse con una frecuencia alta, puede suponer un coste elevado para la organización.

166. Para automatizar la revisión de los registros y la generación de alertas ante parámetros anómalos la organización debe evaluar la necesidad de integrar una herramienta LFM (*Log File Monitor*) de detección de intrusos a nivel de host con el entorno de correo

corporativo. Estas herramientas generarán, ante entradas anómalas en los registros, alertas de seguridad dirigidas en tiempo real al personal responsable de su análisis en cada caso y evitarán que un atacante logre modificar o eliminar registros del servidor para ocultar sus actividades (por supuesto, los registros significativos deberán ser enviados en cada alerta al sistema centralizado de recepción). También debe evaluarse la posibilidad de realizar análisis estadísticos sobre los registros, ya en modo batch, para detectar desviaciones significativas con respecto a valores medios en la organización, indicativas habitualmente de anomalías o posibles problemas de seguridad.

167. Independientemente de qué revisiones se planteen, de cómo se ejecuten las mismas y de con qué periodicidad se realicen, en caso de detectar anomalías en los registros del sistema o aplicación, se debe notificar inmediatamente al departamento de seguridad de la organización, si no es éste el que realiza dichas revisiones, con objeto de emprender las acciones pertinentes en cada caso.

2.6. AUDITORÍA TÉCNICA

168. Como el resto de elementos del entorno TIC corporativo, los sistemas involucrados en la gestión del correo electrónico deben ser analizados técnicamente por un equipo de seguridad independiente de los administradores de sistemas o redes; para ello debe establecerse una política de auditorías técnicas que contemple tanto el análisis automático como las pruebas manuales y por supuesto el seguimiento de las acciones de mitigación sobre los riesgos asociados a las vulnerabilidades lógicas de los sistemas.

169. Por motivos obvios de costes, las pruebas automáticas pueden ser ejecutadas con una frecuencia alta o muy alta (típicamente, una vez por semana), planificando las mismas para que los informes generados por las herramientas de análisis sean procesados, de una u otra forma, por el equipo de seguridad de la organización.

170. Estas pruebas automáticas deben ser obligatoriamente complementadas con análisis manuales ejecutados por el equipo de seguridad corporativa con una menor frecuencia, a determinar por la organización en cada caso (típicamente se realizan cada mes o cada trimestre, en función de la profundidad de análisis requerida y los recursos disponibles para la auditoría). Adicionalmente, al menos una parte de los elementos implicados en la gestión del correo corporativo –por ejemplo, el servidor SMTP de la organización- va a tener visibilidad desde Internet, por lo que es importante realizar los análisis no solo desde los equipos de la organización, sino también desde Internet, determinando así la visibilidad que del entorno poseería un atacante externo y las posibles vulnerabilidades que podrían ser aprovechadas por este.

171. Es necesario que cada organización evalúe la necesidad de complementar los análisis técnicos que realiza el equipo de seguridad interno con análisis ejecutados por equipos ajenos completamente a la organización con una periodicidad determinada (anual o bienal, típicamente); estos análisis suelen ser más profundos e ir dirigidos a entornos concretos, en este caso a los elementos que gestionan el correo corporativo (aunque podría ampliarse a más infraestructura TIC), también con una visibilidad al menos externa de los sistemas de correo. Una buena aproximación puede ser el lanzamiento de un test de penetración que trate de obtener acceso a información corporativa albergada en el entorno de correo de la organización.

2.6.1. METODOLOGÍA DE AUDITORÍA

172. La organización debe implantar una metodología de auditoría de aplicación tanto para los análisis ejecutados por el equipo de seguridad de la propia organización como para los análisis ejecutados –al menos a nivel de directrices generales- por equipos de seguridad externos a ésta. Para el análisis técnico global de seguridad del entorno de correo electrónico, una buena aproximación de mínimos, sin menoscabo de otras cualesquiera que cada organización considere, puede basarse en OSSTMM, contemplando al menos los siguientes módulos:

173. Inspección de red.

174. Identificación de servicios

175. Identificación de aplicaciones

176. Identificación de sistemas

177. Identificación y verificación de las vulnerabilidades.

178. Nivel de filtrado.

179. Sistemas de detección de intrusos.

180. Seguridad de las contraseñas

181. Análisis de la arquitectura de red.

182. En el caso particular del análisis de seguridad de aplicaciones web que proporcionen acceso al correo corporativo los análisis anteriores deben complementarse con los derivados del framework de auditoría web OWASP, contemplando al menos las tareas descritas a continuación:

183. Recopilación de información.

184. Pruebas de gestión de configuración de la infraestructura.

185. Comprobación del sistema de autenticación.

186. Gestión de las sesiones.

187. Gestión de las autorizaciones.

188. Comprobación de la lógica de negocio.

189. Validación de los datos de entrada.

190. Todo el proceso de auditoría debe ser trazado y convenientemente documentado por el equipo analista, tanto si se trata de equipos internos a una organización como si se trata de equipos externos, y debe realizarse en contacto continuo con los responsables de la plataforma de correo corporativo en cada caso. Independientemente del tipo de análisis, un problema habitual en muchas organizaciones es la ausencia de planes de seguimiento de las acciones emprendidas para mitigar los riesgos determinados en una auditoría. Es obligatorio que el personal de seguridad corporativa, dentro de la metodología de análisis a implantar, defina los procedimientos necesarios para el seguimiento y control de las acciones derivadas de un análisis técnico, de forma que se confirme que los riesgos hallados durante la auditoría son correctamente tratados por parte de las áreas implicadas en cada caso.

3. SEGURIDAD DEL CLIENTE DE CORREO

3.1. EQUIPOS DE USUARIO

191. Para garantizar la seguridad del correo electrónico corporativo, como elemento clave en el flujo de mensajes, es necesario garantizar la seguridad de los equipos de usuario utilizados para procesar dicho correo. Para ello, se debe bastionar el equipo de usuario de forma adecuada, sea cual sea su sistema operativo, teniendo en cuenta, sin menoscabo de otros cualesquiera, los siguientes extremos:

192. Actualización correcta del sistema operativo en cuanto a releases y parches de seguridad. Debemos garantizar que tenemos notificación de nuevas actualizaciones por parte del fabricante, y que éstas se incluyen en la política de P&V correspondiente, tal y como se ha indicado con anterioridad para los servidores de correo.

193. Utilización de herramientas antimalware en el equipo. Siempre que técnicamente sea posible, debe considerarse obligatorio el uso de antivirus corporativo en los equipos de usuario, y mantener las bases de datos de patrones víricos correctamente actualizadas. El software antivirus debe disponer de capacidad para detectar y eliminar otro tipo de *malware*, o en su defecto complementar dicho software con herramientas ad hoc para evitar la presencia de troyanos, gusanos, adware, etc., con especial atención a las herramientas de captura de teclados (*keyloggers*).

194. Restricciones de acceso. El usuario, en su trabajo habitual, no debe disponer de privilegios de root o administrador. Adicionalmente, las sesiones deben bloquarse de forma automática tras un periodo de inactividad de quince minutos, tal y como se indica a continuación.

195. Los equipos especialmente relevantes, por ejemplo los correspondientes a personal que por su trabajo pueda manejar información sensible o disponer de privilegios en el entorno tecnológico, deben ser objeto de especial monitorización y control.

196. La organización debe evaluar la conveniencia de utilizar cortafuegos en los equipos personales, tanto desde el punto de vista de seguridad como desde el punto de vista funcional.

197. El equipo personal, fuera de los horarios de trabajo, debe permanecer apagado salvo necesidad estricta y justificada que indique lo contrario.

198. Si el equipo de usuario almacena correo electrónico, es necesario analizar la conveniencia de cifrar el directorio donde se ubiquen los mensajes; esta conveniencia debe considerarse obligatoria en equipos portátiles, debido a la mayor probabilidad de robo o pérdida de los mismos.

199. Las salvaguardas de índole tecnológica, como las expresadas a continuación, deben ser complementadas con medidas de protección física en relación a los equipos de usuario; en especial, la organización debe implantar una política de mesas limpias que obligue al personal a mantener su puesto de trabajo despejado y con la información mínima para el desempeño del trabajo en cada momento ([mp.eq.1]) y debe establecerse un control técnico de bloqueo de los equipos ([mp.eq.2]) que obligue al usuario a autenticarse de nuevo en el sistema tras un periodo de inactividad máximo de quince minutos.

200. Estas normas, y otras relativas a seguridad y bastionado de los equipos de usuario, deben ser incluidas en la normativa de uso de equipos personales de una organización, ya que todos ellos suelen ser utilizados para la gestión del correo electrónico corporativo. Adicionalmente a cualquier normativa o política escrita, la organización debe auditar el cumplimiento de las directrices de seguridad en equipos de usuario –incluyendo dispositivos portátiles- de forma periódica, mediante muestreo significativo de los equipos corporativos. En el caso particular de dispositivos portátiles será además de aplicación lo especificado en la medida de protección [mp.eq.3] del Esquema Nacional de Seguridad, en función del nivel de la información almacenada en el equipo, haciendo especial hincapié en la obligatoriedad de, en el caso de información de nivel alto, cifrar los datos almacenados en el dispositivo (portátil, teléfono móvil, etc.).

3.2. CLIENTES DE ESCRITORIO

201. Como el resto de aplicaciones de los equipos de usuario, los MUA instalados en dichos equipos deben estar permanentemente actualizadas a su última versión, al menos en cuanto a parches de seguridad, así como correctamente configuradas; es necesario destacar que las configuraciones que presentan estas aplicaciones por defecto, al ser instaladas, suelen considerarse inseguras, por lo que la organización debe, en función del cliente de correo corporativo, definir las directrices de configuración segura de dicho cliente, aplicarlas en todos los casos y verificar que se mantienen de forma correcta en el tiempo.

202. Cada vez más clientes de escritorio para la gestión del correo electrónico permiten la interpretación de contenido activo, desde JavaScript hasta ActiveX, por citar unos ejemplos, así como la carga de contenidos remotos en los mensajes de correo. Es obligatorio desactivar estas características en los clientes de cualquier tipo, ya que en caso contrario se introducen riesgos innecesarios en la organización, tanto relativos a malware y ataques dirigidos como relativos a la confidencialidad de la información.

203. De la misma forma, debe considerarse obligatoria la desactivación de acciones automáticas del cliente sobre el contenido de los mensajes de correo, como la vista previa, la apertura o la carga de imágenes –incluidas remotas- en los mismos. Estas funcionalidades introducen riesgos innecesarios en la organización, ya que diferentes ataques pueden ser ejecutados a partir de dichas acciones automáticas del cliente de correo, sin ningún tipo de intervención humana.

204. En el caso de clientes de correo que incorporen capacidades antispam –incluyendo antiphising- o equivalentes, es necesario que la organización analice dichas capacidades y establezca las directrices de configuración segura necesarias en cada caso; si los mensajes sospechosos son almacenados por el cliente de correo en una carpeta determinada –configuración habitual-, el contenido de dicha carpeta debe ser revisado periódicamente para confirmar que es correcto y completo, lo que permitirá por un lado detectar problemas de funcionamiento (en especial, marcado incorrecto) y por otro amenazas dirigidas contra la organización o un usuario en particular. La organización debe evaluar desde todos los puntos de vista, en especial el legal y el operativo, quién debe ejecutar dichas revisiones: generalmente será el propio usuario el responsable de las mismas, por lo que se le deben facilitar directrices de revisión y, en especial, un servicio de notificación de situaciones anómalas para que el área de seguridad corporativa pueda ser avisado e intervenir en caso necesario.

3.3. CLIENTES MÓVILES

205. Es cada vez más habitual que las organizaciones proporcionen servicios de correo electrónico a través de dispositivos móviles (teléfonos inteligentes, agendas electrónicas…). Estos elementos, desde el punto de vista de seguridad, pueden considerarse sistemas y aplicaciones de usuario, por lo que todas las restricciones comentadas con anterioridad (bastionado, actualización de software, configuración correcta…) son de aplicación para estos dispositivos.

206. Estos dispositivos introducen en la organización una serie de riesgos asociados a la movilidad; de esta forma, además de los controles habituales de seguridad –equivalentes como hemos indicado a los aplicables a sistemas de usuario-, en el caso de dispositivos móviles la organización debe considerar las salvaguardas adecuadas desde el punto de vista físico, como la correcta protección frente a robos o pérdidas, así como restricciones desde el punto de vista lógico. Entre ellas es necesario aplicar las siguientes medidas:

207. Control de acceso al dispositivo mediante contraseña. El uso del dispositivo debe requerir una clave previa a cada utilización; dicha clave es independiente del PIN solicitado al arrancar el dispositivo, y deberá introducirse antes de acceder a agenda, contactos, tareas, etc. La organización debe **descartar** el uso de dispositivos que no permitan implantar este control de acceso.

208. Cifrado de la información almacenada. Si el dispositivo móvil presenta capacidad de cifrado de los datos almacenados en él, tanto en memoria interna como en tarjetas de expansión, la organización debe evaluar la necesidad de aplicar esta característica en los dispositivos corporativos, evitando así que un atacante con acceso físico al dispositivo pueda extraer estos datos. En el caso de personal que por su trabajo esté manejando información sensible, el cifrado del dispositivo debe considerarse obligatorio.

209. Cifrado de la información transmitida. La organización debe evaluar la necesidad de que los dispositivos móviles utilizados para la gestión del correo corporativo incorporen capacidades de cifrado y firma digital de los mensajes, así como de que soporten protocolos de transporte y acceso seguros a los servidores de correo corporativo (POP, IMAP, SMTP).

210. Borrado seguro. Los dispositivos móviles utilizados para la gestión del correo corporativo deben soportar el borrado seguro de su información y configuraciones, tanto de forma local, con acceso físico al dispositivo (por ejemplo antes de que el mismo pueda ser transferido a otra persona de la organización) como de forma remota, por ejemplo ante un robo o pérdida del dispositivo.

211. Sistemas de control de software dañino. Si técnicamente es posible, la organización debe implantar controles para reducir los riesgos asociados al software dañino en los dispositivos móviles, en especial sistemas antivirus.

212. En función del tipo de dispositivo móvil corporativo (BlackBerry, iPhone…), la organización debe definir las directrices de bastionado y configuración segura correspondientes, velando por la aplicación de las mismas y su correcto mantenimiento en el tiempo. De la misma forma, si el dispositivo es susceptible de gestionar información sensible, la organización debe evaluar la conveniencia de limitar o directamente eliminar el uso del protocolo 2G por parte de dicho dispositivo, ya que este protocolo presenta vulnerabilidades conocidas que podrían permitir a un atacante interceptar la información transmitida.

3.4. CLIENTES WEB

213. Al igual que en el resto de aplicaciones de los equipos de usuario, y tal y como se ha indicado para los clientes de escritorio, los navegadores utilizados para acceder a correo vía web deben estar permanentemente actualizados a su última versión, al menos en cuanto a parches de seguridad, así como correctamente configurados. En el caso de los navegadores esta necesidad es mucho más dura que en otras aplicaciones, ya que un navegador incorrectamente actualizado o configurado en un equipo puede ser una vía de entrada para muchas amenazas a la seguridad corporativa, desde malware a robos de datos o incluso el control total de un sistema.

214. Es obligatorio que una vez ha finalizado la sesión web, el usuario desconecte del servidor mediante un proceso que elimine la posibilidad de reutilización de la sesión cerrada. Para ello, el servidor web debe ofrecer un modo de desconexión segura accesible por el usuario, así como implantar políticas correctas de caducidad de las sesiones, cerrándolas automáticamente tras un periodo de inactividad.

215. La organización debe analizar las características de seguridad de los navegadores utilizados a nivel corporativo, comprobar que son acordes a los requisitos de seguridad establecidos y, si es técnicamente posible, forzar una configuración segura para todos los usuarios, sin posibilidad para éstos de modificarla sin la correspondiente autorización. Debe establecerse en cualquier caso un proceso de auditoría periódica, por ejemplo mediante muestreo, para garantizar que los niveles de seguridad establecidos se mantienen en el tiempo de forma correcta y completa. Las directrices de seguridad en los navegadores deben contemplar al menos los siguientes extremos:

216. Desactivación de la interpretación de contenidos remotos a la hora de leer mensajes de correo vía webmail, para evitar problemas de malware, ataques dirigidos o confidencialidad de la información, tal y como se ha indicado en los clientes de escritorio.

217. Desactivación de las características de recordar contraseñas para el navegador.

218. Borrado automático, al cerrar el navegador, de la información sensible registrada por el mismo: histórico de navegación, histórico de descargas, histórico de formularios, caché, *cookies*, contraseñas (independientemente de la desactivación de la característica indicada con anterioridad), sesiones autenticadas, etc.

219. Instalación de *addons* para el navegador prohibida o, al menos, notificación al usuario en caso de intento de instalación de un *addon*.

220. Como en la mayor parte de situaciones, estas directrices de configuración deben ir acompañadas de la información o formación correspondiente a los usuarios, así como de mecanismos de notificación ágil al Departamento de Seguridad corporativo en caso de anomalías que puedan ser representativas de un riesgo para la organización.

3.5. ACCESO SEGURO AL SERVIDOR

221. Tanto POP3 como IMAP transfieren información en claro entre el servidor de correo y el cliente utilizado por el usuario, por lo que un tercero podría realizar ataques de interceptación de los datos transmitidos a través de estos protocolos. Por este motivo, las organizaciones deben evaluar la posibilidad de utilizar POP3S e IMAPS, que no son más que la denominación habitual de los protocolos clásicos POP3 e IMAP pero a través de túneles de cifrado SSL; de esta forma se evitan riesgos asociados a la interceptación de datos; si la información que se transmite es sensible, el uso de estos protocolos seguros debe considerarse obligatorio en la organización.

222. Para poder utilizar POP3S e IMAPS se requiere tanto de una configuración determinada en el servidor de correo, para poder entender dichos protocolos mediante la generación de los certificados correspondientes –fuera del objeto de la presente guía-, como de un cliente capaz también de entender ambos protocolos (en la actualidad, la mayor parte de MUA los soportan de manera estándar). Con la configuración adecuada de ambos extremos los usuarios, de forma transparente, podrán gestionar su correo electrónico con un nivel adicional de seguridad al ofrecido por POP3 e IMAP.

223. En el caso de acceso vía web al correo electrónico, tal y como se ha indicado con anterioridad, debe considerarse obligatorio el uso de SSL/TLS tanto para la autenticación del usuario como para la sesión en general. Es necesario recordar que estos protocolos proporcionarán seguridad en la comunicación entre el usuario y el servidor, pero no en la transmisión del correo a su destinatario. Por este motivo, debe considerarse adicionalmente la necesidad de cifrar o firmar el mensaje, tal y como se indica en el punto siguiente de la presente guía, y de establecer protocolos de acceso seguros entre el servidor web y el MTA corporativo.

Nota: no todos los entornos de correo web soportan la integración con sistemas de cifra o firma digital; en estos casos será necesario cifrar o firmar el mensaje mediante una aplicación externa e incorporar el correo cifrado como un anexo al mensaje o pegando directamente dicho texto cifrado –en el caso de salida en formato ASCII- en el cuerpo del correo electrónico.

224. Independientemente del tipo de cliente utilizado en cada caso (escritorio, móvil…) es necesario deshabilitar, como se ha indicado con anterioridad, las características relativas a recordar contraseñas por parte de la aplicación, que la mayor parte de MUA o navegadores web incorporan. El introducir una clave de forma manual para acceder al correo electrónico –al menos en el primer inicio de sesión- debe considerarse obligatorio en cualquier tipo de organización.

225. Si el acceso al correo electrónico se produce desde equipos ajenos a la organización (típicamente accesos desde Internet), en especial a través de navegadores web, debe considerarse obligatorio que el usuario verifique que las características de seguridad del navegador son aceptables, en particular las referentes a recordar contraseñas y a borrado de cookies; en cualquier caso, volvemos a insistir en que proporcionar este tipo de accesos es un riesgo muy considerable para la organización, ya que el equipo cliente, no controlado, puede estar comprometido y por tanto la información que trata puede ser interceptada independientemente de la configuración de un navegador o MUA concretos, por lo que es necesario evaluar muy cuidadosamente si permitimos estos accesos ([op.acc.7]).

4. SEGURIDAD DEL CONTENIDO

4.1. CIFRADO Y FIRMA DE DATOS

226. El contenido de un mensaje de correo electrónico viaja, desde su emisor hasta su receptor, en texto claro; esto significa que un atacante que intercepte un mensaje, en cualquiera de los sistemas por los que pasa el mismo entre emisor y receptor, podrá acceder tanto a su contenido como a sus cabeceras. Generalmente, no será posible –en entornos habituales- cifrar las cabeceras de un correo, por lo que tendremos que asumir el riesgo de que la información contenida en éstas sea interceptada –no suele ser información crítica, sino datos técnicos de servidores intermedios, horas y demás-. Por el contrario, la información más relevante, la potencialmente sensible, irá en el cuerpo del mensaje, en forma de texto, ficheros adjuntos, etc. Si en cualquier caso quisiéramos cifrar toda la comunicación, deberíamos acudir a soluciones VPN o equivalentes, utilizadas casi en exclusiva entre un número limitado de organizaciones y que garantizan la confidencialidad no sólo del cuerpo y los anexos de un mensaje, sino también de sus cabeceras.

227. Independientemente de soluciones basadas en VPN, poco implantadas, la información a la que hacíamos referencia, la contenida en el cuerpo del mensaje, es la que podemos y, en muchos casos, debemos, proteger de ataques de interceptación. Para ello debemos cifrar convenientemente dicha información, medida de protección obligatoria en el caso de entornos de nivel alto ([mp.info.3]), bien mediante herramientas integradas en los clientes de correo, bien mediante herramientas independientes –adjuntando en este caso el archivo cifrado como un fichero más en nuestro mensaje-.

228. Existen herramientas de cifrado de clave pública ampliamente utilizadas capaces de integrarse con múltiples clientes de correo electrónico, lo que hace sencillo su uso, y que permiten no sólo el cifrado sino también la firma de los mensajes, tanto desde el propio cliente como en línea de órdenes. Las organizaciones deben analizar la conveniencia de implantar controles y herramientas para el cifrado (y firma) del correo electrónico de acreditada robustez, que empleen algoritmos acreditados por el Centro Criptológico Nacional y preferentemente productos certificados ([op.pl.5]) en el caso de entornos de nivel alto. Siempre que sea posible se deben escoger herramientas integradas con los clientes de correo corporativos, de forma que se facilite al usuario la gestión segura de su correo desde el propio MUA, sin necesidad de herramientas externas. Ejemplos de estas herramientas pueden ser PGP o su variante de código abierto GPG.

229. La mayor parte de aplicaciones de cifra, como las indicadas con anterioridad, soportan tanto el uso de claves privadas como el de claves públicas. En un esquema de clave privada, la clave de cifrado y la de descifrado coinciden y deben ser conocidas por emisor y receptor; si se transmite la clave a través de canales inseguros, como el correo electrónico, podemos introducir un riesgo no asumible, por lo que habitualmente se suele comunicar la contraseña mediante telefonía o mecanismos equivalentes. Esto no es aceptable en comunicaciones regulares de información sensible, ya que estos medios de transmisión para la contraseña no garantizan un nivel de seguridad adecuado. Por este motivo debemos utilizar esquemas basados en criptografía de clave pública.

230. En la criptografía de clave pública no es necesario el intercambio previo de claves secretas para poder descifrar un mensaje o un fichero adjunto, basta con disponer de la clave pública del receptor para cifrar el mensaje y, una vez recibido, sólo el receptor

podrá descifrarlo con su clave privada. Estos esquemas suelen introducir también la capacidad de firma digital, de forma que el emisor de un correo electrónico no sólo cifra su contenido sino que además lo firma, garantizando así la confidencialidad, la integridad y el no repudio de los datos. Desde herramientas sencillas, como PGP/GPG, hasta complejas infraestructuras de clave pública (PKI), existen una multitud de mecanismos para incorporar criptografía de clave pública con firma y cifrado en las organizaciones, por lo que debemos evaluar las necesidades corporativas en cada caso e implantar soluciones que se ajusten a dichas necesidades de seguridad en el correo electrónico.

231. El cifrado por sí mismo garantiza un cierto nivel de privacidad, en función del esquema de cifra utilizado y del producto que lo implanta, aceptable en la mayor parte de ocasiones, pero no garantiza otros aspectos críticos para la seguridad del correo electrónico, como la autenticación emisor/receptor, la integridad de los datos o el no repudio. Por este motivo cualquier sistema de seguridad en el correo electrónico debe incorporar no sólo la cifra de la información, sino además la firma de ésta, sin importar su nivel de seguridad ([mp.info.4]). Así, el emisor de un correo electrónico no sólo debe cifrar su contenido, sino que para incrementar la seguridad de los datos debe firmarlo, de manera que el receptor por un lado descifra la información (confidencialidad) y por otro, gracias a la firma digital, verifica que el receptor es quien dice ser y el contenido del correo es íntegro. Todo ello en un proceso muy transparente para el usuario final, y por lo general mediante herramientas directamente integradas en los MUA que no requieren de dicho usuario ni conocimientos especiales ni un esfuerzo adicional en la gestión del correo. Por este motivo, cualquier organización que requiera de unos mínimos mecanismos de seguridad en el correo electrónico debe implantar obligatoriamente elementos de firma digital, con los requisitos marcados por el ENS en la medida de seguridad identificada como [mp.info.4] de dicho Esquema.

232. En cualquier caso es necesario tener siempre en consideración en las políticas y normativas de seguridad corporativa, en relación al cifrado de datos en el correo electrónico, los siguientes aspectos:

233. Las cabeceras de un correo electrónico, en términos generales, no pueden ser cifradas, por lo que un ataque de interceptación puede tener acceso a estos datos, que en ocasiones proporcionan información técnica significativa.

234. En especial el asunto de un correo con información sensible no debe proporcionar información significativa del contenido, ya que este es un campo que no se cifrará habitualmente.

235. Si ciframos un fichero adjunto con un programa que añada una extensión al nombre del fichero, un ataque de interceptación puede tener acceso a dicho nombre, por lo que debemos utilizar nombres de archivo poco significativos o incluso completamente asépticos: aa.doc, 123.xls…

236. El uso de criptografía de clave privada no es aceptable para correspondencia electrónica habitual debido a las potenciales debilidades en la transmisión de la clave, por lo que debemos implantar y utilizar un esquema basado en criptografía de clave pública.

237. El cifrado de los datos por sí mismo no garantiza la autenticidad del emisor si no va acompañado de firma digital, por lo que no debemos considerar válida cualquier información que nos llegue simplemente cifrada.

4.2. CONTROL DEL CORREO NO CORPORATIVO

238. Tal y como se ha indicado en la introducción del presente documento, es muy habitual que las personas dispongan de más de una cuenta de correo; típicamente se dispondrá de cuentas corporativas, asociadas al puesto de trabajo, y de cuentas personales, asociadas al ámbito privado de las personas. Con frecuencia, los usuarios acaban utilizando, al menos esporádicamente, ambos tipos de direcciones de correo electrónico para ambos propósitos, lo que puede repercutir negativamente en la seguridad de la información.

239. El uso del correo corporativo con fines personales no suele implicar problemas de seguridad relevantes salvo en casos aislados. De cualquier forma, es necesario que la política corporativa de uso del correo electrónico indique que el uso del correo con fines personales sea razonable, y por supuesto que no viole ninguno de los principios expuestos en dicha política: debemos tener presente que la imagen de las personas que componen una organización es en parte la imagen de sus empleados, por lo que una degradación de ésta puede implicar un riesgo reputacional para la propia organización. Dicho de otra forma, el uso del correo corporativo con fines personales que puedan degradar la imagen, por cualquier motivo, de la organización, debe ser algo expresamente prohibido en la política de uso del correo electrónico corporativo.

240. En cualquier caso, es mucho más preocupante el uso del correo personal con fines profesionales; aquí solemos encontrar dos situaciones diferenciadas, en función de la intencionalidad del uso:

241. **Uso malintencionado.** Un usuario puede utilizar un servicio de correo externo a la organización, típicamente un webmail, para robar datos corporativos, por ejemplo enviando la información desde un correo externo a otro, también externo, fuera del control de la organización. Realmente, dicho usuario podría utilizar su cuenta corporativa para realizar este robo de información, pero los posibles controles implantados en los sistemas de correo de la organización podrían llegar a detectarlo, con lo que se suele utilizar un servicio externo.

242. **Uso bienintencionado.** Un usuario se envía información corporativa a sí mismo, utilizando como origen su cuenta de correo en la organización (escenario habitual) y como destino su cuenta de correo personal con una buena intención. Típicos ejemplos de esta situación se producen para poder trabajar en casa con informes, documentos, etc. En este caso, se introduce un riesgo significativo porque estamos enviando información potencialmente sensible a servidores fuera del control de la organización, incluso ubicados en terceros países.

243. Para mitigar los riesgos asociados a las situaciones anteriores, es necesario en primer lugar prohibir expresamente en la política de seguridad corporativa el uso de direcciones de correo personales para la gestión de información sensible; esto será el respaldo corporativo a cualesquiera medidas técnicas que la organización implante.

244. Adicionalmente a esta salvaguarda organizativa, la organización debe evaluar la conveniencia de denegar técnicamente la conexión de la organización con los webmails habituales (Hotmail, GMail, etc.), mediante la implantación de reglas adecuadas en los cortafuegos perimetrales de la organización. Por supuesto, esto mitiga el riesgo pero no lo elimina, ya que actualmente, en especial para un uso malintencionado, un usuario puede utilizar múltiples servicios de correo web y es prácticamente imposible filtrar el acceso a todos ellos (aún así, podría instalar un servidor propio con un sistema de correo web accesible a través del protocolo HTTP, con lo que en la mayor parte de cortafuegos o

proxies simplemente se detectarían conexiones mediante este protocolo, habitualmente permitidas en cualquier organización). Para evitar el uso de los protocolos web en puertos no estándar (es decir, diferentes del 80/tcp o del 443/tcp) la organización debe restringir el tráfico saliente desde su plataforma, permitiendo por defecto únicamente el tráfico con destino estos puertos estándar.

245. También es necesario evaluar la posibilidad de monitorizar el tráfico saliente por los protocolos habituales en el uso de webmails, típicamente HTTP y HTTPS; el comportamiento habitual de ambos protocolos es enviar unos pocos datos –solicitudes- y a cambio recibir una cantidad de información considerablemente mayor a la enviada, por lo que si la organización es capaz de detectar cantidades anómalas de tráfico saliente HTTP o HTTPS puede encontrarse ante una potencial fuga de información.

4.3. TÉCNICAS ANTIMALWARE

246. Tal y como se ha indicado con anterioridad, el correo electrónico es hoy en día un mecanismo de difusión de software dañino ampliamente utilizado. Por este motivo, es obligatorio instalar en nuestro entorno herramientas capaces de detectar y eliminar el software malicioso enviado a través de mensajes de correo, con independencia de la categoría del sistema ([op.exp.6]).

247. Debemos implantar sistemas de protección tanto en los servidores de correo u otros elementos intermedios (cortafuegos, pasarelas, *relays*…) como en los equipos de usuario donde se ubican los clientes; ambos elementos son críticos para la seguridad corporativa, ya que en los primeros debemos poder detener correos potencialmente peligrosos antes que puedan llegar a sus destinatarios, mientras que los segundos son el punto último de protección frente a este tipo de mensajes (por ejemplo, recibidos ante un funcionamiento anómalo del servidor que los debía haber detenido o simplemente cifrados y sin posibilidad de ser leídos en el servidor). La organización debe considerar obligatorio, en cualquier caso, el uso de al menos dos niveles de protección frente a software dañino (servidor de correo y equipo de usuario) y, si es posible, el uso de productos de diferente fabricante en cada uno de estos puntos.

248. En cualquier caso, es obligatorio que la organización conciencie a los usuarios en general sobre la importancia de su actitud a la hora de evitar ataques víricos, en particular en relación a la no apertura de archivos adjuntos provenientes de fuentes no confiables, a la no ejecución de archivos sospechosos independientemente de su fuente (por ejemplo, aquellos con dos extensiones identificadas como peligrosas) o a la no apertura de correos anómalos de fuentes aparentemente confiables (por ejemplo, correos de compañeros de trabajo en lenguaje no habitual).

249. Independientemente de cualquier salvaguarda técnica, si los usuarios no cumplen estas directrices es muy probable que se materialicen incidentes relativos a difusión de software dañino en la organización. Adicionalmente, como en otros casos, la organización debe proporcionar a sus usuarios mecanismos de reporte de alertas o anomalías que puedan suponer potenciales riesgos para la seguridad de la información corporativa, haciendo que estas alertas lleguen al personal de la organización con capacidad para mitigar dichos riesgos en un tiempo mínimo.

4.3.1. PROTECCIÓN EN ELEMENTOS INTERMEDIOS

250. Los sistemas antivirus de correo (aunque genéricamente se les denomine así, estas herramientas tienen capacidad de detectar y bloquear no sólo virus, sino además otros tipos de malware) deben instalarse en el servidor o servidores corporativos o en elementos de transporte intermedios como los citados con anterioridad; su administración rutinaria incluye la actualización periódica del software y, especialmente, de las firmas de patrones víricos (como en cualquier entorno antivirus), pero dada la criticidad de los sistemas que gestionan el correo de la organización, estas actualizaciones deben complementarse con pruebas manuales también periódicas –y a ser posible, automatizadas- para confirmar que el sistema funciona correctamente y es capaz de detener malware dirigido contra la organización. Las pruebas de funcionamiento periódicas deben incluir:

251. Comprobación de la correcta actualización del software, confirmando que la herramienta antivirus está actualizada a su última *release*. Con frecuencia las nuevas versiones de las herramientas introducen características de seguridad o de funcionalidad que, salvo excepciones, son importantes para cualquier organización.

252. Comprobación de la correcta actualización de las firmas de virus, confirmando que la base de datos de patrones víricos está actualizada a su última versión. Esto permitirá a la organización detectar los nuevos virus que a diario se generan en todo el mundo sin que éstos lleguen a afectar a la seguridad corporativa.

253. Prueba EICAR. Se trata de un test para comprobar que el antivirus está correctamente integrado con el sistema de transferencia de correo, mediante el envío de una cadena de texto determinada guardada en un fichero aparentemente ejecutable (extensión .exe, .com…). El antivirus debe generar una alerta ante el envío de este archivo, completamente inofensivo pero que permite comprobar que el sistema está levantado y funcionando correctamente. Es importante destacar que la prueba EICAR es un test antiguo y conocido por los fabricantes antivirus, por lo que debe ejecutarse únicamente como confirmación de que el sistema está funcionando correctamente e integrado en el MTA, no como garantía de actualización de la base de datos de patrones víricos.

254. El sistema antivirus de correo debe ser capaz de eliminar los correos que contengan adjuntos con extensiones potencialmente peligrosas (típicamente, .EXE, .VBS, .BAT, .DLL, .DEV…); esta medida permite a la organización ignorar los adjuntos sospechosos y por tanto reducir el riesgo de difusión, ya que los ficheros potencialmente maliciosos pero no identificados por la base de datos de patrones víricos no llegarán a su receptor. Así, debe considerarse un simple punto de partida necesario, pero no una salvaguarda que evite el análisis completo de los ficheros adjuntos dado que un atacante puede alterar la extensión del archivo dañino sin modificar su peligrosidad, puede ofuscar este código malicioso a través de múltiples mecanismos y, en especial, cada vez es más habitual el malware empotrado en ficheros ofimáticos que, probablemente, y desde un punto de vista organizativo, no podrán ser detenidos en el servidor.

255. De esta forma, el antivirus de correo debe no sólo ser capaz de detectar ficheros adjuntos con extensiones peligrosas sino además, y mucho más importante, analizar dichos ficheros para, con independencia de su extensión, poder detectar código malicioso en los mismos y eliminarlo sin que llegue a su receptor. Esta capacidad, presente en cualquier antivirus de correo de los múltiples existentes, ve reducida su efectividad si los anexos o

el cuerpo completo de un mensaje de correo electrónico va cifrado y no puede ser descifrado en el propio servidor (situación habitual), por lo que en este caso el único análisis válido será el ejecutado por el antivirus instalado en el equipo del propio usuario.

4.3.2. PROTECCIÓN EN EQUIPO DE USUARIO

256. En el caso de los antivirus denominados personales, aquellos instalados en los equipos del usuario final, la organización debe seleccionar un único producto antivirus a nivel corporativo de la amplia variedad existente en el mercado. Dicho producto debe ser adecuado a las necesidades de la organización en materia de seguridad y, en especial, debe disponer de una política de actualizaciones muy frecuente para evitar que la base de datos de patrones víricos pueda quedar obsoleta. Desde un punto de vista técnico, el usuario no debe, en ningún caso, ser capaz de alterar el correcto funcionamiento del sistema antivirus de su equipo, por ejemplo deshabilitando características de análisis o deteniendo la ejecución de la aplicación; las actualizaciones de firmas deben estar programadas de forma automática y, de la misma forma, el usuario no debe tener la capacidad de alterar su funcionamiento.

257. En el caso de uso de webmails externos a la organización es vital el correcto funcionamiento de este antivirus instalado en el equipo final, ya que en este caso, si está permitido el acceso, no entran en juego los antivirus de correo corporativos, únicamente los posibles sistemas de filtrado de contenidos web o equivalentes.

258. Algo similar sucede a la hora de analizar mensajes cifrados –bien los anexos o bien el cuerpo completo-, tal y como se ha indicado previamente; en este caso, los elementos intermedios no tienen capacidad de análisis, o no suelen tenerla, ya que no son capaces de descifrar la información del mensaje para poderla analizar limitándose entonces bien a bloquear directamente cualquier mensaje no analizado –lo que evita que correos legítimos lleguen a su destinatario- o bien a dejarlos pasar –permitiendo que software dañino incorporado a dichos mensajes llegue al usuario final-. De esta forma, como se ha indicado con anterioridad, es crítico el correcto funcionamiento del entorno antivirus instalado en el equipo del usuario.

4.4. TÉCNICAS ANTISPAM

259. De la misma forma que para el software malicioso que pueda sernos remitido a través del correo electrónico, es obligatorio utilizar tecnologías que eviten que el correo no deseado (correo basura, SPAM) llegue a nuestros buzones, tanto a nivel de servidor de correo o elementos intermedios como a nivel de cliente.

260. Habitualmente, los sistemas de filtrado de SPAM trabajan en base a modelos heurísticos, por lo que es posible que puedan llegar a detener correo legítimo (falso positivo) o a transmitir correctamente SPAM (falso negativo). Ambas situaciones suponen un potencial problema para nuestra seguridad, ya que por un lado podemos estar bloqueando correo relevante dirigido hacia nuestra organización y por otro podemos estar entregando a nuestros usuarios correo basura también dirigido a nosotros.

261. Un caso particular de SPAM es el llamado *phishing* (del término inglés *fishing*, pesca). El phishing es una estafa cometida a través del correo electrónico en la que, mediante técnicas de ingeniería social, el atacante trata de obtener datos confidenciales de un usuario de forma fraudulenta. Los ataques de phishing más habituales hoy en día son los orientados a la obtención de credenciales para accesos bancarios a través de Internet, en

los que simulando un correo legítimo de una entidad financiera se dirige a la víctima a una web fraudulenta que simula ser la de dicha entidad, para una vez allí solicitarle, típicamente con la excusa de verificación de la seguridad, sus credenciales de acceso. Una vez robadas ("pescadas") dichas credenciales, el atacante podrá realizar movimientos bancarios a través de Internet suplantando la identidad de su víctima.

262. Como en el caso de las técnicas antimalware, es obligatorio que la organización conciencie a los usuarios en general sobre la importancia de su actitud a la hora de evitar ataques relativos al SPAM, en particular en relación a la solicitud de información personal –especialmente datos financieros en ataques de phishing- y a la no respuesta, bajo ningún concepto y a través de ningún medio (fax, teléfono, correo…), a un correo electrónico sospechoso de ser SPAM. De la misma forma que en el caso del malware, si los usuarios no cumplen estas directrices es muy probable que se materialicen incidentes relativos a difusión de correo no deseado en la organización, con independencia de sus salvaguardas técnicas.

4.4.1. PROTECCIÓN EN ELEMENTOS INTERMEDIOS

263. Adicionalmente al modelo heurístico implantado en los sistemas antispam corporativos, en casi todos estos sistemas se permite la definición de listas blancas (direcciones de correo o dominios completos desde los que los mensajes directamente se consideran legítimos, sin atender a criterios adicionales) y listas negras (direcciones de correo o dominios completos desde los que, por el contrario, todos los mensajes se consideran no deseados). Es obligatorio en todos los entornos la implantación de al menos el primer elemento (listas blancas), para evitar la pérdida de mensajes que, bajo criterios heurísticos, pudieran ser catalogados como SPAM sin serlo realmente.

264. En el caso de las listas negras, la organización debe evaluar la conveniencia de implantar controles en los elementos intermedios de transporte del correo que bloqueen todo el correo electrónico proveniente de direcciones o dominios incluidos en dichas listas. Actualmente, la mayor parte de MTA soportan esta característica, siendo en cualquier caso necesaria una reconfiguración del servidor y un proceso de alimentación y actualización de las listas (RBL, DNSBL, RHSBL...).

265. Debemos analizar, en cada caso, si podemos permitirnos el bloqueo o incluso el borrado de un mensaje legítimo en nuestras organizaciones, catalogado como SPAM sin serlo realmente; si no es así, una configuración que podemos utilizar es el marcado del correo como no deseado en base a sus características ponderadas, por ejemplo incluyendo un nuevo campo en la cabecera de cada mensaje, sin bloqueo o eliminación en el servidor. De esta forma, cada usuario podrá habilitar reglas de filtrado de mensajes en su cliente de correo, por ejemplo para dirigir aquellos mensajes cuya probabilidad de ser SPAM supere un umbral a una determinada carpeta, carpeta que el usuario revisará periódicamente según sus necesidades.

4.4.2. PROTECCIÓN EN EQUIPO DE USUARIO

266. Cada vez más clientes de correo electrónico incorporan capacidades antispam empotradas en el propio MUA, con independencia de las reglas de filtrado de mensajes en base a características de su cabecera o cuerpo indicadas con anterioridad. La organización debe evaluar la conveniencia de aplicar estas capacidades en los equipos de usuario mediante políticas centralizadas y preferiblemente comunes a toda la organización. Estos sistemas

funcionan de forma equivalente a los sistemas antispam ubicados en elementos de transporte intermedios, mediante modelos heurísticos que, en base a características de los mensajes y a un proceso de aprendizaje, son capaces de, con una alta probabilidad, identificar y marcar el correo considerado SPAM.

267. A diferencia del caso de protección frente a malware en el equipo de usuario, en el que la implantación de controles antivirus o equivalentes es obligatoria en cualquier caso, en la protección frente a correo no deseado en el equipo de usuario la organización, como se ha indicado previamente, debe evaluar las necesidades corporativas en materia de seguridad y los beneficios e inconvenientes de implantar estas capacidades.

268. También a diferencia de la protección frente a malware en el equipo final, en la que un sistema antivirus es capaz de analizar los mensajes de correo electrónico –o intercambio de información en general- desde un punto de vista global, en el caso de las técnicas antispam del MUA éstas no serán efectivas para el correo procesado de forma alternativa, típicamente a través de webmails. En este caso, la organización debe evaluar, como se ha indicado con anterioridad, la conveniencia de permitir o denegar estos accesos y, en caso de que se decida permitirlos, aplicar controles que eviten que el SPAM, en especial el relativo a ataques de phishing, pueda llegar a su destinatario.

ANEXO A. CHECKLISTS

Se presentan en este anexo las listas de comprobación de los diferentes controles y directrices expuestos en esta guía. Dichas listas deben considerarse como una base de auditoría para la configuración de un entorno de correo seguro, pero no como una guía de auditoría por sí mismas, ya que no detallan aspectos necesarios para un análisis real, como fechas, responsables de mitigación, controles compensatorios, evidencias, etc.

A.1. ORGANIZACIÓN

#ID	Control	Estado
#1	Se ha ejecutado un análisis de riesgos en base a las directrices del ENS que abarque los servicios de correo electrónico	
#2	Existe una política de seguridad corporativa definida en la organización	
#3	Existe una normativa de uso del correo electrónico definida en la organización	
#4	La normativa definida recoge los extremos indicados en la guía en relación a deberes y obligaciones	
#5	Existen directrices o recomendaciones de uso del correo electrónico definidas y publicadas en la organización	
#6	La organización ha analizado formalmente los requisitos de seguridad corporativos del servicio de correo teniendo en cuenta los factores expuestos en la presente guía	
#7	Existe una segregación de tareas adecuada para la gestión del correo electrónico corporativo	

A.2. SEGURIDAD DEL SERVIDOR

#ID	Control	Estado
ARQUITECTURA		
#1	Los sistemas de transporte o entrega de correo están ubicados en una zona de red adecuada	
#2	La red está protegida adecuadamente mediante sistemas cortafuegos	
#3	[ALTO] Se utilizan dos sistemas cortafuegos en cascada, de diferente fabricante y con alta disponibilidad	
#4	El control de tráfico de transporte y entrega de correo es adecuado en el cortafuegos	
#5	La organización ha evaluado convenientemente la posibilidad de denegar el tráfico SMTP saliente, con excepción de los MTA corporativos	
#6	[ALTO] Existen entornos IDS/IPS para detectar o detener ataques contra el entorno de correo corporativo	
#7	[ALTO] Los registros de IDS/IPS se analizan correctamente	
BASTIONADO		
#8	El bastionado de servidores y aplicaciones de correo se realiza en base a las guías STIC correspondientes siempre que éstas existan	
#9	Los sistemas de correo están en entornos dedicados y con software mínimo instalado en los mismos	

BASTIONADO: P&V		
#10	La organización ha definido y aprobado una política P&V que contemple los aspectos establecidos en la presente guía	
#11	La organización dispone de un inventario de sistemas, aplicaciones, configuraciones… de los elementos intervinientes en la gestión del correo corporativo.	
#12	El inventario anterior se actualiza convenientemente	
#13	La organización obtiene información de seguridad correcta y completa de los fabricantes, proveedores, etc. de los elementos intervinientes en la gestión del correo corporativo	
#14	Ante la recepción de información de seguridad, ésta es convenientemente analizada por la organización	
#15	La organización está en disposición de obtener parches y actualizaciones de seguridad de sus proveedores	
#16	Los parches y actualizaciones se aplican de forma adecuada para garantizar el mínimo impacto en la organización	
#17	Los parches y actualizaciones se verifican una vez implantados para confirmar que corrigen las vulnerabilidades identificadas en cada caso	
BASTIONADO: SERVICIOS		
#18	Los servicios de red no necesarios para el funcionamiento de la plataforma de correo han sido deshabilitados	
BASTIONADO: CONTROL DE ACCESOS		
#19	El cortafuegos corporativo bloquea o permite tráficos en base a las directrices expuestas en la guía	
#20	La organización ha evaluado convenientemente las salvaguardas relativas a control de acceso de sistemas y aplicaciones, y las implanta de forma adecuada	
BASTIONADO: AUTENTICACIÓN		
#21	Se han eliminado los usuarios de aplicación o sistema no necesarios para el correcto funcionamiento de la plataforma de correo electrónico	
#22	Los accesos administrativos al servidor se realizan mediante usuario nominal	
#23	Si existen cuentas de servicio o sistema que no pueden ser eliminadas pero no requieren inicios de sesión interactivos, éstas han sido convenientemente restringidas	
#24	Las políticas de contraseñas están aplicadas sobre los entornos de correo siempre que técnicamente sea posible	
#25	Las políticas de contraseñas generan claves robustas	
#26	La organización ha evaluado la conveniencia de bloquear un acceso tras un número determinado de conexiones erróneas	
BASTIONADO: PERMISOS		
#27	Los permisos a nivel de sistema de ficheros para los buzones de correo garantizan que únicamente su propietario podrá acceder a los mismos	
#28	La organización ha evaluado convenientemente la posibilidad de utilizar buzones de correo cifrados	
#29	El acceso privilegiado a los servidores de correo está restringido a las personas necesarias en cada caso	
#30	[MEDIO, ALTO] Las acciones de los administradores de sistemas son registradas y revisadas mensualmente por el Departamento de Seguridad	
MONITORIZACIÓN Y CONTROL		
#31	Los sistemas que gestionan el correo corporativo son convenientemente monitorizados	
#32	La organización ha evaluado convenientemente la necesidad de monitorizar accesos a determinados buzones de correo	

#33	Los elementos de control son analizados por personal independiente de la administración del servidor	
SERVICIOS DE CORREO		
#34	La versión de las aplicaciones de correo es correcta y se actualiza convenientemente	
#35	La configuración de las aplicaciones de correo es correcta y se verifica convenientemente	
#36	El acceso a los servicios de correo está restringido a los orígenes estrictamente necesarios	
#37	El riesgo asociado al acceso a los servicios de correo desde Internet ha sido convenientemente analizado	
#38	Se verifica periódicamente que el MTA corporativo no actúa como *Open Relay*	
#39	En el caso de proporcionar acceso web al correo corporativo la organización ha implantado salvaguardas para evitar los ataques más habituales a estos entornos	
#40	En el caso de proporcionar acceso web al correo corporativo el servidor web no está ubicado en el propio MTA	
#41	En el caso de proporcionar acceso web al correo corporativo las comunicaciones se realizan mediante protocolos cifrados	
#42	En el caso de proporcionar acceso web al correo corporativo se proporcionan mecanismos de terminación automática de la sesión tras un periodo de inactividad	
ADMINISTRACIÓN DEL SERVIDOR		
#43	La administración del servidor se basa en procedimientos documentados y aprobados por la organización	
#44	Existe una segregación de funciones adecuada para la administración de los servicios de correo	
#45	La administración remota del servidor se realiza mediante protocolos cifrados	
#46	La administración remota del servidor se realiza desde orígenes restringidos por IP	
#47	La administración remota del servidor requiere autenticación robusta	
#48	La administración remota del servidor se realiza mediante usuarios nominales que ejecutan tareas administrativas con privilegios exclusivamente cuando es necesario	
ADMINISTRACIÓN: COPIAS DE RESPALDO		
#49	La organización ha definido una política de copias de respaldo que ha sido aprobada y cuyo cumplimiento se audita periódicamente	
#50	La organización ha definido una política de restauraciones periódicas y la ejecuta satisfactoriamente, cumpliendo los supuestos indicados en la presente guía	
#51	Los medios de copia de respaldo disponen de medidas de protección aceptables en cualquier caso	
#52	Los medios de copia de respaldo están convenientemente etiquetados según las directrices de la presente guía	
#53	La custodia de medios de copias de seguridad se realiza contemplado las salvaguardas definidas en la presente guía	
#54	[MEDIO, ALTO] Los medios móviles de copia de respaldo están cifrados	
#55	En el caso de transporte de medios se contemplan las salvaguardas definidas en la presente guía	
ADMINISTRACIÓN: GESTIÓN DE USUARIOS		
#56	Existe un procedimiento formalmente definido en la organización para la identificación de usuarios que contemple las directrices expuestas en la presente guía	

#57	[ALTO] El acceso a los sistemas se produce mediante autenticación robusta	
#58	Los derechos de acceso a los entornos de correo se basan en el principio de mínimo privilegio	
#59	La organización ha definido quién posee la capacidad de conceder, alterar o anular autorizaciones de acceso y cómo debe hacerlo, aplicando dicho esquema de forma ágil	
#60	La organización ha implantado una política de revisiones periódicas, al menos mensuales, de usuarios en el servidor de correo que contempla las directrices expuestas en la presente guía	
ADMINISTRACIÓN: CONTINUIDAD DEL SERVICIO		
#61	La organización ha realizado un análisis de impacto que identifica requisitos de disponibilidad y qué sistema son críticos para la prestación del servicio de correo electrónico	
#62	[MEDIO, ALTO] Los RTO del servicio de correo electrónico están identificados y aprobados por la organización	
#63	[ALTO] La organización ha desarrollado un plan de continuidad para el servicio de correo electrónico, cubriendo los aspectos especificados en el ENS	
#64	[ALTO] La organización ejecuta pruebas de continuidad del servicio de correo electrónico al menos una vez al año	
REGISTROS Y AUDITORÍA		
#65	La organización ha evaluado convenientemente las capacidades de seguridad, en especial en lo relativo a registros de auditoría, de la plataforma de correo corporativa	
#66	[MEDIO, ALTO] El registro de actividades de usuario se realiza según las directrices expuestas en el ENS	
#66	Los registros del sistema están convenientemente protegidos	
#67	[ALTO] Los registros del sistema están protegidos según los términos definidos en el ENS	
#68	Se aplican marcas de tiempo para los registros según las directrices definidas en el ENS	
#69	Los relojes de los sistemas de correo están convenientemente sincronizados	
#70	Los registros de auditoría se procesan en busca de anomalías o violaciones de seguridad en los términos especificados en la presente guía	
#71	La revisión de registros es periódica y acorde a las necesidades corporativas de seguridad	
#72	Existe un proceso de notificación al personal correspondiente de cualesquiera anomalías detectadas en las revisiones de registros	
AUDITORÍA TÉCNICA		
#73	La plataforma de correo electrónica es auditada técnicamente por personal independiente de su administración	
#74	Se realizan análisis automáticos y pruebas manuales con una periodicidad definida y aprobada en la organización	
#75	La organización ha implantado una metodología de auditoría de sistemas y la aplica contra la plataforma de correo electrónico, en los términos definidos en la presente guía	
#76	En el caso de ofrecer correo vía web, la organización ha implantado una metodología de auditoría de aplicaciones web y la aplica contra la plataforma de correo electrónico, en los términos definidos en la presente guía	
#77	Todo el proceso de auditoría es trazado y documentado	
#78	La organización ha definido los procedimientos necesarios para el seguimiento y control de las acciones derivadas de una auditoría	

A.3. SEGURIDAD DEL CLIENTE

#ID	Control	Estado
EQUIPOS DE USUARIO		
#1	Los equipos de usuario están correctamente actualizados en cuanto a parches de seguridad	
#2	Los equipos de usuario disponen de herramientas antimalware siempre que técnicamente sea posible, correctamente implantadas y actualizadas	
#3	Los usuarios trabajan habitualmente bajo la premisa del mínimo privilegio	
#4	Las sesiones de los equipos de usuario se bloquean tras un periodo de inactividad de 15 minutos	
#5	Los equipos especialmente relevantes son monitorizados y controlados convenientemente	
#6	La organización ha evaluado la necesidad de implantar cortafuegos personales en los equipos de usuario	
#7	Fuera del horario de trabajo los equipos personales permanecen apagados salvo necesidad estricta y justificada	
#8	La organización ha evaluado la necesidad de cifrar los mensajes de correo almacenados en los equipos de usuario	
#9	En el caso de equipos portátiles, la organización ha implantado esquemas de cifrado de la información almacenada en los sistemas	
#10	La organización ha implantado una política de mesas limpias para los usuarios	
#11	La organización ha definido una normativa de uso de equipos personales, que es aplicada y auditada convenientemente	
CLIENTES DE ESCRITORIO		
#12	Los MUA están convenientemente configurados y actualizados en parches de seguridad	
#13	La organización ha analizado las directrices de configuración segura del MUA corporativo, las aplica en todos los casos y verifica que se mantienen en el tiempo	
#14	La interpretación de contenido activo está desactivada en los clientes de correo en todos los casos	
#15	Las acciones automáticas del MUA sobre los mensajes están desactivadas en todos los casos	
#16	Si el MUA incorpora capacidades antispam, la organización debe establecer convenientemente las directrices de configuración y uso de las mismas	
CLIENTES MÓVILES		
#17	La organización aplica las directrices correctas de seguridad en equipos de usuario sobre los dispositivos móviles	
#18	Los dispositivos móviles requieren, en todos los casos, una clave de acceso previa a cada utilización	
#19	La organización ha evaluado convenientemente la necesidad de cifrar la información ubicada en los dispositivos móviles, debiendo considerar obligatoria la cifra en el caso de información sensible	
#20	La organización ha evaluado convenientemente la necesidad de cifrar los mensajes en tránsito desde los dispositivos móviles, así como de proveer protocolos de acceso y transporte seguros	
#21	Cualquier dispositivo móvil utilizado para el acceso al correo corporativo debe proporcionar capacidades de borrado seguro, tanto local como remoto	
#22	Si técnicamente es posible, la organización debe implantar controles de software dañino para los dispositivos móviles	
#23	La organización ha definido las directrices de bastionado y configuración para los dispositivos móviles corporativos, aplicándolas convenientemente y	

	auditándolas en el tiempo	
#24	La organización ha evaluado la conveniencia de deshabilitar el uso del protocolo 2G en los dispositivos móviles que gestionen información sensible	
CLIENTES WEB		
#25	Los navegadores utilizados para el acceso al correo vía web están convenientemente configurados y actualizados desde el punto de vista de seguridad	
#26	El servidor de correo web implanta mecanismos de desconexión y cierre de sesión tanto manuales como automáticos	
#27	Si técnicamente es posible, la organización debe forzar una configuración segura de los navegadores sin posibilidad de ser modificada de forma no autorizada	
#28	Se auditan periódicamente el cumplimiento y aplicación de las directrices de seguridad en navegadores definidas en la organización	
#29	Los navegadores utilizados para la gestión del correo vía web tienen desactivada la interpretación de contenidos remotos	
#30	Los navegadores utilizados para la gestión del correo vía web tienen desactivada la característica de recordar contraseña	
#31	Los navegadores utilizados para la gestión del correo vía web borran automáticamente la información sensible al ser cerrados	
#32	Los navegadores utilizados para la gestión del correo vía web no permiten la instalación desatendida de *addons*	
#33	Los usuarios han sido convenientemente formados en el uso seguro del navegador para acceso al correo corporativo, disponiendo de canales ágiles de notificación de anomalías que puedan implicar un riesgo	
ACCESO SEGURO		
#34	La organización ha evaluado convenientemente la necesidad de utilizar POP3S e IMAPS para acceso seguro al correo	
#35	En el caso de acceso vía web, la sesión completa se realiza siempre mediante SSL/TLS	
#36	El acceso al correo siempre requiere de una contraseña introducida en cada caso por el usuario de forma manual	
#37	La organización ha evaluado convenientemente la necesidad de acceder al correo corporativo desde Internet y es consciente de los riesgos que estos accesos implican	

A.4. SEGURIDAD DEL CONTENIDO

#ID	Control	Estado
CIFRADO Y FIRMA		
#1	[ALTO] La información que se transmite por correo electrónico siempre viaja cifrada	
#2	La organización ha evaluado la necesidad de implantar controles de cifrado y firma de acreditada robustez para el intercambio de correo electrónico	
#3	[ALTO] Los productos de cifra para el correo electrónico están certificados por el CCN	
#4	En el intercambio habitual de información sensible se utiliza siempre cifrado de clave pública	
#5	La organización ha evaluado convenientemente las necesidades corporativas en materia de cifrado y ha implantado soluciones acordes a dichas necesidades	
#6	La organización ha incorporado firma digital al correo electrónico en los términos definidos por el ENS	
#7	Se han facilitado a los usuarios directrices de seguridad a considerar en el	

	envío de correo electrónico cifrado/firmado, cubriendo al menos los términos expuestos en la presente guía	
CORREO NO CORPORATIVO		
#8	La normativa de uso del correo electrónico especifica las condiciones de uso de direcciones de correo no corporativas	
#9	El uso del correo corporativo con fines personales que puedan degradar la reputación de la organización está expresamente prohibido en la normativa correspondiente	
#10	La normativa de uso del correo electrónico prohíbe expresamente el uso de correo personal para la gestión de información sensible	
#11	La organización ha evaluado convenientemente la posibilidad de prohibir, desde un punto de vista técnico, el acceso a los webmails habituales	
#12	La organización ha evaluado convenientemente la posibilidad de monitorizar el tráfico saliente para detectar posibles fugas de información a través del correo electrónico	
TÉCNICAS ANTIMALWARE		
#13	La organización dispone de herramientas capaces de detectar y eliminar el código dañino y las implanta y utiliza de forma adecuada	
#14	Las herramientas de control de software dañino están convenientemente implantadas tanto en los equipos de usuario como en los elementos intermedios de la plataforma de correo	
#15	La organización ha concienciado a sus usuarios en un uso seguro del correo electrónico que evite la infección por malware	
#16	La organización proporciona mecanismos de alerta y respuesta ante potenciales incidentes de seguridad relativos a correos dañinos	
#17	La organización comprueba periódicamente la correcta actualización del software antimalware en servidores de correo	
#18	La organización comprueba periódicamente la correcta actualización de las firmas de patrones víricos en servidores de correo	
#19	La organización comprueba periódicamente la correcta integración del software antimalware y el software de aplicación en servidores de correo	
#20	El sistema antimalware del servidor de correo es capaz de eliminar adjuntos que contengan extensiones potencialmente peligrosas	
#21	El sistema antimalware del servidor de correo es capaz de analizar adjuntos y cuerpo de los mensajes en busca de patrones de malware	
#22	Los antivirus en equipo de usuario se actualizan periódica y automáticamente	
#23	Los usuarios no tienen capacidad para alterar el correcto funcionamiento de los sistemas antimalware instalados en sus equipos	
TÉCNICAS ANTISPAM		
#24	La organización dispone de herramientas capaces de detectar y eliminar el correo no deseado y las implanta y utiliza de forma adecuada	
#25	La organización ha concienciado a sus usuarios en un uso seguro del correo electrónico que evite ataques derivados del correo no deseado, en especial los relativos a fuga de información o *phishing*	
#26	Los sistemas antispam ubicados en elementos de la plataforma de correo corporativo soportan el uso de listas blancas	
#27	La organización ha evaluado convenientemente la utilización de listas negras para evitar correo no deseado	
#28	La organización ha evaluado convenientemente la posibilidad de eliminar el correo considerado SPAM o simplemente marcarlo como tal	
#29	La organización ha evaluado convenientemente la posibilidad de aplicar capacidades antispam en los MUA si técnicamente es posible	
#30	En el caso de aplicar capacidades antispam en los MUA, la organización ha definido e implantado las directrices adecuadas en cada caso	

ANEXO B. CÓDIGO DE BUENAS PRÁCTICAS

En este anexo se facilita un código de buenas prácticas en la gestión del correo electrónico a modo de resumen de los apartados y directrices expuestos en la presente guía. Se ha estructurado en tres grandes apartados, en función de a qué conjunto de personas van dirigidas las recomendaciones y buenas prácticas: administradores de la plataforma de correo (típicamente, áreas como Sistemas o Comunicaciones), administradores de seguridad (típicamente, el departamento de Seguridad corporativa) y, finalmente, usuarios del correo electrónico, personal de la organización que usa el servicio de correo para su trabajo habitual y que es un punto clave en la seguridad global.

B.1. ADMINISTRADORES DE PLATAFORMA

La plataforma de correo está ubicada en una zona desmilitarizada de la red y protegida convenientemente por los cortafuegos corporativos.

Los flujos de tráfico en relación a la plataforma de correo son los mínimos imprescindibles.

El tráfico SMTP saliente de la organización se restringe al MTA corporativo.

Existen sistemas de detección o prevención de intrusiones y sus registros son analizados en tiempo real para detectar anomalías.

Los servidores de correo están correctamente bastionados y se aplican correctamente parches y actualizaciones de seguridad.

Las contraseñas de los sistemas y aplicaciones son robustas.

Tras un número determinado de conexiones erróneas se genera una alerta dirigida al área de Seguridad.

La plataforma de correo se monitoriza para detectar tanto incidencias funcionales como de seguridad.

El servidor de correo no actúa como relay abierto.

No se permite el acceso desde Internet al correo corporativo, salvo a través de VPN.

Se han implantado protocolos de acceso seguro al servidor: POP3S, IMAPS y HTTPS, y se fuerza a los usuarios a su utilización.

Los procedimientos operativos de administración están correctamente documentados.

La plataforma de correo está incluida en una política de copias y restauraciones que permiten recuperar la información en un tiempo acotado.

Los medios de copia están protegidos frente a intrusiones.

Los usuarios de la plataforma se gestionan mediante procedimiento formal y se revisa mensualmente que son correctos y completos.

Los sistemas y aplicaciones generan registros de auditoría y éstos se analizan para detectar anomalías.

Los relojes de los sistemas de la plataforma están sincronizados.

Los equipos cliente están actualizados y disponen de antivirus.

Los equipos cliente se bloquean automáticamente tras 15 minutos de inactividad.

Los equipos cliente permanecen apagados fuera del horario de trabajo.

Se ha definido una política de mesas limpias.

B.2. ADMINISTRADORES DE SEGURIDAD

Debemos definir una política de seguridad corporativa en la organización, que se especifique en diferentes normativas de seguridad, entre ellas la de uso del correo electrónico.

Debemos realizar un análisis de riesgos en base a las directrices del ENS que identifique amenazas, probabilidades, impactos y riesgos sobre el servicio de correo electrónico.

Debemos definir y difundir directrices o recomendaciones de uso del correo electrónico seguro para los usuarios, directas y sin entrar en detalle técnico, que reflejen y resuman la normativa de uso aceptable del correo. La difusión debe ser periódica.

Las tareas de gestión de las plataformas de correo electrónico deben estar segregadas correctamente.

Debemos definir procedimientos de auditoría que cubran los siguientes aspectos:

Plataforma de correo corporativo, tanto desde Internet como desde la propia organización.

Puestos de usuario (mesas limpias, equipos correctamente configurados, apagados fuera de horario, etc.).

Dispositivos móviles y equipos portátiles, prestando especial atención al cifrado de datos.

Las auditorías deben lanzarse de forma periódica y las acciones derivadas de cada una de ellas deben ser convenientemente trazadas para garantizar que se aplican salvaguardas en los casos en los que sea necesario.

B.3. USUARIOS

Las contraseñas de acceso a los recursos corporativos son personales e intransferibles, por lo que deben mantenerse en secreto.

Está prohibida la instalación y ejecución de software que no sea indispensable para el correcto desempeño de las tareas asignadas en la organización.

No debemos ejecutar ningún fichero descargado desde Internet o recibido por correo electrónico u otros medios no confiables.

Queda expresamente prohibido el uso del correo electrónico corporativo para la difusión de mensajes racistas, violentos, xenófobos u ofensivos de cualquier forma.

Queda expresamente prohibido el uso de direcciones de correo personales para el envío de información sensible.

Política de mesas limpias: no debemos dejar físicamente accesible ningún tipo de información sensible en los puestos de trabajo.

Si abandonamos nuestro puesto de trabajo, debemos bloquear la sesión o sesiones iniciadas en el equipo.

No debemos responder a ningún mensaje que pueda ser considerado SPAM ni tampoco a hoaxes (bulos) que suelen circular en forma de cadena de correo.

No debemos introducir datos personales, especialmente de banca, en páginas que nos han sido remitidas a través de mensajes de correo electrónico.

Los sistemas antivirus del equipo personal deben estar funcionando correctamente siempre.

En caso de enviar información sensible por correo electrónico debemos cifrarla.

Si sospechamos que se ha producido cualquier violación de la seguridad corporativa o que existe cualquier tipo de debilidad en la misma, debemos notificarlo al área de Seguridad de forma inmediata.

ANEXO C. NORMATIVA DE USO DEL CORREO ELECTRÓNICO

Conforme a la Política de Seguridad Corporativa, la cuenta de correo electrónico que LA ORGANIZACIÓN pone a disposición de sus empleados únicamente podrá ser utilizada para finalidades directamente relacionadas con el desarrollo de las funciones que les corresponden, quedando prohibido el uso de dicha cuenta para fines particulares o ajenos al objeto de su prestación laboral.

En concreto y por lo que respecta al uso del correo electrónico, además de las normas generales de seguridad, el empleado usuario de la cuenta de correo electrónico puesta a su disposición por LA ORGANIZACIÓN queda debidamente informado y deberá tener en cuenta lo siguiente:

El correo proporcionado por LA ORGANIZACIÓN al empleado debe destinarse exclusivamente a un uso profesional, en tanto elemento de trabajo propiedad de LA ORGANIZACIÓN, no pudiendo en consecuencia utilizarse para fines particulares, excepto casos puntuales justificados.

Respecto de cualquier uso particular que el trabajador realice del correo electrónico con carácter puntual y justificado de acuerdo a la norma anterior, el trabajador deberá posteriormente proceder al borrado y destrucción de los mensajes que haya podido enviar y/o recibir sin almacenar copia ni temporal ni definitiva de los mismos.

El empleado realizará en todo caso un uso adecuado, racional y leal del correo electrónico, debiendo utilizarlo en la medida en que resulte necesario para cumplir con las obligaciones concretas de su puesto de trabajo, de conformidad con las reglas de la buena fe y diligencia.

La cuenta de correo electrónico de los trabajadores de LA ORGANIZACIÓN es un instrumento de trabajo y no un instrumento idóneo para las comunicaciones personales. No obstante, LA ORGANIZACIÓN admite que el trabajador pueda hacer un uso racional de esta herramienta informática para fines particulares semejante a la utilización de otros medios más tradicionales como el teléfono, en virtud de su derecho a comunicarse libremente con los demás.

Dicho uso deberá ser en todo caso racional y leal. Consecuentemente, el uso reiterado y abusivo del correo electrónico en horario laboral, para fines particulares y ajenos a la labor profesional del empleado podrá suponer un quebranto de la buena fe contractual así como un abuso de confianza en el desempeño del trabajo, constituyendo un incumplimiento grave y culpable del contrato de trabajo.

Por motivos de seguridad, el correo electrónico no podrá ser utilizado para enviar ni para contestar mensajes o cadenas de mensajes susceptibles de provocar congestiones en los sistemas de LA ORGANIZACIÓN o que puedan introducir malware o implicar cualesquiera riesgos o problemas en los sistemas y herramientas informáticas y tecnológicas de LA ORGANIZACIÓN.

El correo electrónico no podrá ser utilizado con fines comerciales ni lucrativos en beneficio del empleado.

El empleado cuidará en todo momento el lenguaje utilizado en sus comunicaciones, debiendo tener presente que en cada una de ellas compromete la imagen y el nombre de LA ORGANIZACIÓN.

Los contenidos de los correos electrónicos son conservados durante un período de 90 días.

El borrado definitivo de los mensajes electrónicos del servidor se produce a los 120 días.

Una vez extinguida la relación contractual entre el trabajador y LA ORGANIZACIÓN, el trabajador se encargará de eliminar toda aquella información que, ajena a los servicios que haya prestado en LA ORGANIZACIÓN, obre por cualquier causa en su cuenta de correo.

Si un trabajador recibiera en su correo electrónico mensajes con contenido inadecuado deberá poner esta circunstancia en conocimiento de su superior o comunicarlo directamente a las personas responsables de la Dirección de Seguridad para la adopción de las medidas que en su caso resulten pertinentes.

Si un trabajador va a estar ausente en su puesto de trabajo por vacaciones, bajas, excedencias, días voluntarios y/o cualquier otra causa, deberá notificarlo a la dirección del departamento si dicha circunstancia fuera conocida por el trabajador con anterioridad o posteriormente, a los fines de que su correo electrónico sea redireccionado a una cuenta del departamento de otro compañero o del director con el fin de que pueda ser aperturado y en su caso atender las gestiones de trabajo que al mismo se correspondan. Además, tanto el trabajador como en su caso el administrador de los correos, activará como acuse de recibo para los remitentes de los mensajes una comunicación en la que se indique que el destinatario del correo se encuentra ausente y en su lugar el mensaje de correo electrónico será abierto y contestado por otro empleado de la entidad.

ANEXO D. NORMATIVA DE IDENTIFICACIÓN Y AUTENTICACIÓN

Nota: se marcan en *cursiva* aspectos no recogidos obligatoriamente en el ENS y que deben considerarse simples ejemplos, a sustituir por los establecidos en cada organización.

La normativa de identificación y autenticación de LA ORGANIZACIÓN define la correcta identificación de los usuarios de la información y de los elementos tecnológicos que la soportan, su autenticación con respecto a ellos y las responsabilidades derivadas del acceso a los recursos corporativos; todo lo que no esté explícitamente permitido en esta normativa, se considera prohibido (ISO/IEC 27002, Código de buenas prácticas para la Gestión de la Seguridad de la Información, 9.1.1.2).

La **identificación** de cada usuario ante un activo de LA ORGANIZACIÓN debe ser unívoca, su uso se considera personal y exclusivo, y es responsabilidad única del usuario el mantenimiento en secreto de cualquier código que posibilite el acceso a un recurso corporativo. El identificador de usuario ha de ser único dentro de LA ORGANIZACIÓN y estará formado por *la inicial del nombre seguida del primer apellido completo*, siempre que no se defina una excepción; en los sistemas cuya tecnología no admita una longitud de nombre suficiente para dar cabida al conjunto, el identificador de acceso se limitará a *la inicial del nombre seguida de tantos caracteres del primer apellido como técnicamente sea posible*.

Se definen como **excepciones** a lo especificado en el párrafo anterior las siguientes:

La existencia previa de un identificador de usuario similar en la organización, en cuyo caso se utilizarán las iniciales del nombre y primer apellido seguidas de tantos caracteres del segundo apellido como técnicamente sea posible.

Los identificadores de usuario definidos con anterioridad a la aprobación de esta política, en cuyo caso se tratará de adaptar los mismos a lo especificado en el presente documento siempre que tecnológicamente sea factible.

Es **obligación** de todo el personal de LA ORGANIZACIÓN el cumplir estrictamente las normas para el uso de contraseñas indicadas a continuación; el personal del Área de Seguridad establecerá los controles técnicos oportunos para verificar tal cumplimiento mediante la prevención y la detección de desviaciones con respecto a la política establecida. Si por cualquier motivo un usuario o grupo de usuarios no pudiera adecuarse de forma correcta a estas normas deberá ponerlo en conocimiento del Área de Seguridad, que aprobará o desestimará los motivos de la desviación.

Se definen los siguientes **tiempos de vida máximos** para todo tipo de claves de acceso a los recursos informáticos de LA ORGANIZACIÓN:

NIVEL ALTO. Treinta días.

NIVEL MEDIO. *Noventa días.*

NIVEL BAJO. Ciento ochenta días.

Adicionalmente, se contemplan al menos los siguientes casos para realizar **cambios extraordinarios** en las contraseñas:

Si alguien con acceso privilegiado a los sistemas de información corporativa abandona LA ORGANIZACIÓN o modifica sus funciones en la misma.

Si se produce un ataque exitoso contra los sistemas corporativos, aunque a priori no afecte directamente a la gestión de contraseñas.

Si existen evidencias de la captura de una o más contraseñas de acceso privilegiado a los sistemas de información corporativos.

Siempre que desde Dirección de Seguridad se considere oportuno.

El **tiempo de vida mínimo** de una clave será *el equivalente a un cuarto del periodo máximo*, excepto si durante ese tiempo se ha de efectuar un cambio extraordinario por cualquiera de los motivos vistos con anterioridad. Si un usuario no cambia su contraseña antes de vencer el tiempo de vida de la misma, o ante una situación de cambio extraordinario solicitada desde el Área de Seguridad o instancias superiores, su acceso será bloqueado y sólo se podrá desbloquear de forma manual por un administrador autorizado y con las garantías de trazabilidad suficientes. En cualquier caso, se implantarán los controles necesarios para notificar una situación de vencimiento del tiempo de vida de una clave con la antelación suficiente para que el usuario interesado pueda modificar su contraseña.

La **longitud mínima** de una clave se fija en *ocho caracteres*, y debe estar formada por números, letras mayúsculas y minúsculas y caracteres de puntuación, incluyendo de forma obligatoria al menos dos letras y un número o signo de puntuación. LA ORGANIZACIÓN pondrá los medios necesarios para forzar a cada usuario o grupo a utilizar este tipo de claves, y adicionalmente controlará la existencia de contraseñas que no cumplan con los requisitos definidos en este documento. Quedan expresamente **prohibidas** las palabras comunes de cualquier lengua, en especial la inglesa y la castellana, así como pequeñas modificaciones de las mismas (por ejemplo, rotaciones o concatenaciones con números de uno o dos dígitos).

El proporcionar deliberadamente acceso a terceros que legítimamente no tengan acceso a los sistemas de información corporativos se considerará una ***falta muy grave***; proporcionar o facilitar el acceso a los sistemas de forma no deliberada a terceros que legítimamente no tengan acceso a ellos se considerará una ***falta grave*** si se considera que no se ha protegido convenientemente la seguridad de dichos accesos.

ANEXO E. GLOSARIO

BIA (*Business Impact Analysis*). Análisis de impacto en el negocio.

ESMTP (*Extended SMTP*). Extensiones al protocolo SMTP.

GPG. Gnu PG. Versión libre –open source- de PGP.

HTTP (*HyperText Transfer Protocol*). Protocolo de transferencia de hipertexto, utilizado habitualmente en navegación web.

IMAP (*Internet Message Access Protocol*). Protocolo de acceso al correo electrónico que mantiene la estructura de carpetas en un servidor centralizado.

MTA (*Mail Transfer Agent*). Agente de Transferencia de correo, ubicado en el servidor.

MUA (*Mail User Agent*). Cliente de correo, ubicado habitualmente en equipos de usuario.

ENS (Esquema Nacional de Seguridad). BOE viernes 29 de enero de 2010.

PGP *(Pretty Good Privacy)*. Software de cifra y firma de datos ampliamente utilizado para reforzar la integridad y confidencialidad de los datos enviados a través de correo electrónico.

POP3 (*Post Office Protocol v3*). Protocolo de descarga de correo desde el MTA hasta el MUA.

RTO (*Recovery Time Objective*). Tiempo en el que es necesario restaurar un determinado servicio tras una parada para que ésta no impacte significativamente en el negocio.

SHTTP (*Secure HyperText Transfer Protocol*). Protocolo de transferencia segura de hipertexto, utilizado habitualmente en navegación web en la que intervenga información confidencial (credenciales de usuario, mensajes de correo electrónico, datos bancarios…).

SMTP (*Simple Mail Transfer Protocol*). Protocolo simple de transferencia de correo, utilizado para el envío de correo electrónico.

SSL (*Secure Sockets Layer*). Protocolo de cifra que permite el intercambio seguro de información entre dos extremos, predecesor de TLS.

TLS (*Transport Layer Security*). Protocolo de cifra que permite el intercambio seguro de información entre dos extremos.

ANEXO F. REFERENCIAS

NIST. Special Publication 800-45 v2. *Guidelines on Electronic mail security*. Febrero, 2007.

Esquema Nacional de Seguridad. BOE del viernes 29 de enero de 2010.

OSSTMM v3. Open Source Security Testing Methodology Manual 3.0. Diciembre, 2010.

OWASP Testing Guide v3. Diciembre, 2008.