MANUAL

Implementación SPF, DKIM y DMARC en servicios públicos

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

Introducción

Más de 700 mil correos maliciosos fueron bloqueados por la Red de Conectividad del Estado el año 2023, como medida preventiva. Esta cifra nos demuestra cuán utilizado es el correo electrónico como vector de entrada para un ciberataque y por qué es tan necesario implementar medidas de seguridad en este canal, como por ejemplo los protocolos de autenticación.

Por esta razón y con el objetivo de contribuir a proteger a las instituciones, el CSIRT de Gobierno desarrolló este manual como guía para implementar de forma efectiva las políticas de autenticación de correo electrónico SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) y DMARC (Domain-based Message Authentication, Reporting, and Conformance) en los servicios públicos.

Estas medidas de seguridad son fundamentales para garantizar la autenticidad y la integridad de los correos electrónicos enviados en nombre de la institución, reduciendo así el riesgo de suplantación de identidad y ataques de phishing.

La información contenida en este documento está orientada a los encargados de ciberseguridad institucionales y a los administradores de sistemas de las unidades TIC, por lo que es necesario contar con conocimientos básicos para su adecuada comprensión y correcta aplicación.

Capítulo 1

Conceptos básicos

Para evitar recibir y enviar correos electrónicos de tipo spam o campañas de phishing, disminuir el riesgo de spoofing y asegurar la entrega de e-mails, existen tres protocolos de autenticación que permiten confirmar que el servidor desde donde se envía un e-mail es seguro.

La implementación de estos protocolos es una medida de seguridad básica para el correo electrónico de las organizaciones. Estos métodos de autenticación son:

¿QUÉ ES SPF?

SPF significa "marco de políticas del remitente". Este protocolo permite identificar o listar los servidores de correo electrónico autorizados por la organización para enviar mensajes desde su dominio, tanto internos como externos. Esto significa que evita que terceros suplanten su dominio de correo electrónico.

¿CÓMO FUNCIONA?

El propietario, encargado de TI o administrador debe crear un registro TXT en el Servidor de Nombres de Dominio o DNS para listar los servidores autorizados para enviar corres electrónico. Si algún servidor no está en la lista, significa que no es un remitente autorizado. Cuando un servidor recibe un mensaje de correo electrónico, realiza una verificación SPF, comprobando si el dominio o IP que envió el correo se encuentra en la lista. Si no es así, la verificación SFP falla, bloquea el mail, envía a spam o permite que ingrese a la bandeja de entrada con una marca, dependiendo de la configuración del receptor en sus equipos de seguridad.

DNS: Servidor que traduce nombres de dominio en direcciones IP para toda la red.

¿QUÉ ES DKIM?

Sus siglas significan claves de identificación de dominio digitales. Se trata de una técnica que utiliza criptografía asimétrica para agregar una firma digital, única a e intransferible, a la cabecera de los correos electrónicos. Gracias a esto, el receptor puede verificar la autenticidad y la integridad del mensaje, y garantizar que no ha sido manipulado entre los servidores de correo.

¿CÓMO FUNCIONA?

Este método requiere agregar un registro TXT en el DNS, con el cual se difunde una clave pública , mientras la llave privada correspondiente se aloja en el servidor de email. Cuando se envía un correo electrónico, el servidor email del remitente firma el mensaje con su llave privada; posteriormente, el servidor email del receptor detecta el DKIM, y utiliza la llave pública contenida en el registro TXT y la cabecera de firma del mensaje para verificar si el este último no fue modificado mientras estuvo en tránsito.

Si el protocolo DKIM reconoce que el correo no fue modificado, se autoriza que llegue a la bandeja de entrada.De lo contrario, el mensaje podría pasar como correo no deseado.

¿QUÉ ES DMARC?

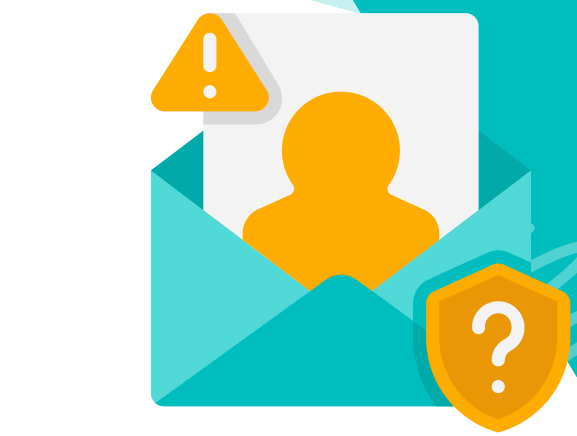
DMARC significa autenticación, informes y conformidad de mensajes basados en dominio. Este protocolo de autenticación ayuda a los proveedores de correo electrónico a identificar mensajes que no provienen de dominios legítimos y especifica cómo se deben gestionar los mensajes que fallan las verificaciones. Por tanto, previene el uso fraudulento de dominios y protege contra el phishing y el spoofing.

DMARC utiliza SPF y DKIM para brindar mayor seguridad y realizar una validación más avanzada. Además, genera reportes que permiten detectar algún problema en la configuración DKIM y SPF.

¿CÓMO FUNCIONA?

La política DMARC, al igual que las anteriores, se debe publicar en el DNS de un dominio como un registro TXT, donde describe su política de autenticación de correo electrónico.

Para configurar este protocolo, es necesario contar con SPF, DKIM, o ambos. Cuando un usuario recibe un correo electrónico, el servidor receptor busca si existe una política DMARC en el DNS, y luego valida la firma DKIM y que la IP coincida con el registro SPF del remitente. Según los resultados, se activará la política DMARC configurada: aceptar, rechazar, marcar como spam, o poner en cuarentena.



Capítulo 2

Preparación para la implementación

Antes de implementar los protocolos SPF, DKIM y DMARC se debe realizar una evaluación del dominio y de los sistemas de correo electrónico, ya que así es posible identificar y corregir cualquier problema de autenticación que pueda afectar la entrega de un mensaje y la seguridad del dominio.

En caso de utilizar plataformas en la nube como Microsoft y Google, se recomienda antes verificar la documentación o contactarse con el proveedor.

Para comenzar, se debe:

- En caso de utilizar plataformas en la nube como Microsoft y Google, se recomienda antes verificar la documentación o contactarse con el proveedor.
- Confirmar que los servidores sean compatibles para realizar este tipo de configuración.
- Comprobar que los sistemas de correo electrónico están monitoreados para detectar posibles problemas de autenticación de correo electrónico.
- Tener acceso y conocimiento para modificar los registros del DNS del dominio sobre el que se encuentra implementado el correo de la institución. Si tu zona DNS es administrada por el Ministerio del Interior, envía un correo a nic@interior.gob.cl para coordinar el trabajo.
- Tener acceso y administración de la plataforma de correos electrónicos y dispositivo de seguridad (antispam) institucionales.
- Identificar si existen servidores tercerizados, y coordinar con los administradores la configuración.

Capítulo 3

Implementación paso a paso

CONFIGURACIÓN SPF

1. Crear un registro TXT en el DNS del dominio desde donde se envía correo electrónico. Esto es: una línea de texto, sin formato y que incorpora mecanismos y valores (IP y nombres de dominio).

Sólo debe haber un registro SPF por dominio y pueden ser de hasta 255 caracteres y no deben pesar más de 512 bytes.

2. Configura el contenido del registro TXT con los siguientes comandos:

Comando	Descripción
v	El registro SPF comienza con este parámetro. Se refiere a la versión de SPF. Es obligatoria y debe configurarse de la siguiente manera: v=spf1
Include	Utiliza el registro SPF de otro dominio como propio: include: interior.gob.cl
a	Permite que los servidores de correo con IP asociada como registro A al domino especificado en este comando puedan enviar un e-mail con el nombre de dominio ingresado: a: interior.gob.cl

Comando	Descripción
mx	Permite que los servidores de correo con IP asociada como registro A al domino especificado en este comando puedan enviar un e-mail con el nombre de dominio ingresado: mx: interior.gob.cl
Ip4 o ip6	Estos mecanismos autorizan a servidores de correos contenidos dentro de una determinada IP o subred.
Exists	Este mecanismo autoriza a servidores de correos electrónicos si existe el dominio indicado en él: Exists: gob.cl
all	Debe ser el último mecanismo del registro SPF. Permite configurar el comportamiento por defecto, en caso de que ninguna otra regla se ejecute.

3 Considera los calificadores para definir las acciones:

Símbolo Configuración	Resultado	Explicación
+	Pass	Indica que el comando especificado en el registro SPF está autorizado para enviar correos electrónicos.
–	Fail	Significa que el comando especificado en el registro SPF no está autorizado para enviar correos electrónicos.
~	Soft Fail	Indica que el comando especificado en el registro SPF es opcional. Esto significa que el servidor puede enviar correo electrónico cumpliendo lo indicado en el comando, pero no está obligado a hacerlo.
?	Neutral	El dominio especificado en el registro SPF no puede ser verificado. Esto ocurre cuando el dominio no tiene un registro SPF o no está bien formado.

4. Validar y confirmar que la configuración esté implementada correctamente.

Ejemplos de implementación

La configuración del SPF dependerá del sistema operativo que se utilice. Supongamos que tenemos una configuración DNS en Linux para el dominio example.com:

```
; Un dominio con dos servidores email, dos
computadores,
; y dos servidores en el dominio example.com
$ORIGIN example.com.
@           MX 10 mail-a
            MX 20 mail-b
            A  192.0.2.10
            A  192.0.2.11
ana         A 192.0.2.65
braulio     A 192.0.2.66
mail-a      A  192.0.2.129
mail-b      A  192.0.2.130
www         CNAME example.com.
; Un dominio relacionado
$ORIGIN example.org.
@           MX 10 mail-c
mail-c      A  192.0.2.140
; Las IP reversas para esas direcciones
$ORIGIN 2.0.192.in-addr.arpa.
10          PTR example.com.
11          PTR example.com.
65          PTR ana.example.com.
66          PTR braulio.example.com.
129         PTR mail-a.example.com.
130         PTR mail-b.example.com.
140         PTR mail-c.example.org.
; Un dominio de IP reversa falso, que dice algo que no
es cierto
$ORIGIN 0.0.10.in-addr.arpa.
4           PTR bob.example.com.
```

Basado en esta configuración se pueden generar los registros SPF que se muestran abajo. Estos ejemplos muestran varios registros publicados posibles para example.com , y qué valores de <ip> harían que el chequeo de SPF fuera positivo. Ten en cuenta que <dominio> es "example.com":

```
v=spf1 +all
   -- Cualquier <ip> pasa el chequeo.
v=spf1 a -all
   -- Las direcciones 192.0.2.10 y 192.0.2.11
pasan el chequeo.
v=spf1 a:example.org -all
   -- Ninguna dirección de salida pasará porque
example.org no tiene registros A.
v=spf1 mx -all
   -- Las direcciones 192.0.2.129 y 192.0.2.130
pasan.
v=spf1 mx:example.org -all
   -- La dirección 192.0.2.140 pasa.
v=spf1 mx mx:example.org -all
   -- Las direcciones 192.0.2.129, 192.0.2.130, y
192.0.2.140 pasan.
v=spf1 mx/30 mx:example.org/30 -all
   -- Cualquier dirección que envía desde
192.0.2.128/30 o 192.0.2.140/30 pasa
v=spf1 ptr -all
   -- La dirección que envía 192.0.2.65 pasa (el
DNS reverso es válido y está en example.com)
   -- La dirección que envía 192.0.2.140 falla (el
DNS reverso es válido pero no está en example.com)
   -- La dirección que envía 10.0.0.4 falla (La IP
reversa no es válida)
v=spf1 ip4:192.0.2.128/28 -all
   -- La dirección que envía 192.0.2.65 falla
   -- La dirección que envía 192.0.2.129 pasa
```

CONFIGURACIÓN DE DKIM [1]

1. Generar claves DKIM. Para esto, puedes utilizar una herramienta como OpenSSL, biblioteca de software de código abierto que se utiliza para generar y administrar claves criptográficas. ¿Cómo hacerlo?

- Abre una terminal y dirígete al directorio donde quieres guardar las claves DKIM.
- Ejecuta el siguiente comando para generar un par de llaves RSA con 2048 bits (a pesar de que parece que se genera sólo la llave privada, en realidad se generan ambas):

```
```
openssl genrsa -out
private.key 2048
```

- Ejecuta el siguiente comando para exportar la clave pública para su uso con DKIM:

```
openssl rsa -in
private.key -out
public.key -outform
PEM -pubout
```

2. Configurar las firmas DKIM en los servidores de correo. Una vez generadas las claves, se deben configurar las firmas DKIM en los servidores de correo que se utilizarán para enviar correo electrónico. Esta configuración variará según el servidor de correo que se utilice, sin embargo, hay que considerar los siguientes parámetros:

Nombre de dominio que se quiere proteger con DKIM
Clave pública DKIM (que se generó en el paso 1)
Política DKIM: Nivel de seguridad que desea implementar con DKIM. Estas políticas son:
```

Política DKIM: Nivel de seguridad que desea implementar con DKIM. Estas políticas son:

Neutral	El correo electrónico que no pasa la autenticación DKIM no se rechazará, pero no se podrá confiar en él.
Soft fail	El correo electrónico no pasa la autenticación DKI, pero se marcará como "no seguro" y se puede entregar, por lo que se debe considerar con precaución.
Hard fail	El correo electrónico que no pasa la autenticación DKIM se rechazará.

3. Publicar la clave pública DKIM en el DNS. Luego de generar el par de llaves, hay que publicar la llave pública en el DNS para que los receptores de correo electrónico puedan verificar la autenticidad de los mensajes. Para realizar este paso, se debe crear un registro TXT en la zona DNS. El registro debe tener el siguiente formato:

```
`v=DKIM1; k=rsa;
p=PUBLIC_KEY
```

Donde:

v	Versión de DKIM
k	Tipo de clave
p	Clave pública

Ejemplo:

Si la clave DKIM es:

```
MIGfMA0GCSqGSIb3DQEB
AQUAA4GNADCBiQKBgQD4
Y+4sA4b016X3n10h6+0+
2v
...
3q9s7r8+wIDAQAB
p=PUBLIC_KEY
```

El registro DKIM sería:

```
v=DKIM1;k=rsa;
p=MIGfMA0GCSqGSIb3DQ
EBAQUAA4GNADCBiQKBgQ
D4Y+4sA4b016X3n10h6+
0+2v
...
3q9s7r8+wIDAQAB
```

CONFIGURACIÓN DE DKIM [2]

Lo primero que se debe hacer antes de configurar DMARC es contar con los protocolos SPF y DKIM activados; de lo contrario, se pueden presentar problemas con la entrega de los correos. Posteriormente, hay que:

1. Generar un registro TXT en el DNS con el siguiente formato:

```
v=DMARC1; p=POLICY;
rua=MAILTO:DMARC_REP
ORT_EMAIL;
ruf=MAILTO:DMARC_REP
ORT_EMAIL
```

Donde:

v	Versión DMARC
p	Política
rua	Dirección de correo electrónico para los informes de DMARC.
ruf	Dirección de correo electrónico para los informes DMARC fallidos

Las políticas disponibles son:

None	El correo electrónico que no pasa la autenticación DMARC se entregará.
Quarantine	El correo electrónico que no pasa la autenticación DMARC se entregará.
Reject	El correo electrónico que no pasa la autenticación DMARC se rechazará.

2 Implementar la política DMARC en los servidores de correo, configurando los servidores de correo para que rechacen, envíen a cuarentena o entreguen el correo electrónico que no pasa esta autenticación. Los parámetros que se deben considerar son:

Política DMARC que se especificó en el registro.

Dominio en el que se configuró la política.

3 Habilitar el envío de informes DMARC. Esta configuración dependerá del servidor de correo que se utilice. No obstante, se deben usar los siguientes parámetros:

Dirección de correo electrónico a la que se enviarán los informes

Dominio para el que se está configurando el envío de informes DMARC

Los informes generados por DMARC son una herramienta muy importante para mejorar la configuración, en caso de ser necesario, e identificar posibles ataques hacia los correos electrónicos, por lo que se recomienda analizarlos regularmente.

Capítulo 4

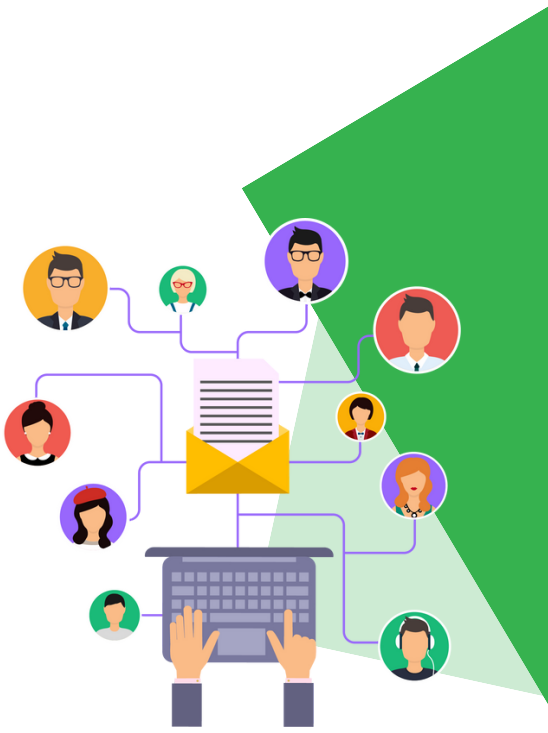
Recomendaciones

El correo electrónico es notablemente difícil de configurar y mantener. Es fácil cometer errores en la configuración, y dado que los cambios tienen que propagarse a través del sistema de nombres de dominio, a veces es necesario esperar varias horas para que una modificación se haga efectiva. Además, el correo electrónico no viaja encriptado por defecto.

Dado todo lo anterior, la principal recomendación que tenemos es no usar correo electrónico si es posible usar otro medio de comunicación. Por ejemplo, si se trata de un equipo de trabajo dentro de un departamento o división, o incluso dentro de la institución completa, aplicaciones simples como WhatsApp o Signal, o más complejas y completas como Slack, Mattermost, Discordo Zulip (considerando el resguardo de la confidencialidad de la información en cada caso), permiten hacer todo lo que se hace con correo electrónico y mucho más. Sin embargo, puesto que el correo electrónico todavía es muy prevalente entre instituciones, te recomendamos lo siguiente cuando lo configures para tu institución:

- Analiza los informes que genera DMARC, ya que permite:
  - Identificar intentos de suplantación de identidad.
  - Detectar si existe un aumento de los correos electrónicos no autenticados, signo de que el correo electrónico está siendo atacado.
  - Saber si existe un incremento de los correos que no son validados por SPF o DKIM.
  - Implementar medidas de seguridad de forma oportuna.

- Comprueba que los servidores de correo electrónico cuenten con el protocolo SPF correctamente configurado.
- Revisa que los sistemas de correo electrónico estén configurados para aplicar correctamente las políticas DMARC.
- Ajusta las políticas SPF, DKIM y DMARC a las necesidades y realidad de la organización. Crea un plan para aplicar los ajustes necesarios y hacer revisiones.
- Implementa gradualmente estos protocolos para minimizar las interrupciones e identificar a tiempo algún problema.
- En caso de cambiar de proveedor, dominios o servidores de correo electrónico, se deben actualizar correspondientemente los valores configurados para el uso de los protocolos SPF y DKIM.
- Para mayor seguridad del dominio, puedes cambiar la política DKIM a “Hard Fail”, de forma que los correos que fallen esta verificación sean siempre rechazados.
- Para evitar interrupciones de servicio de correo electrónico por problemas de configuración, informa a la organización cualquier cambio en las políticas, especialmente si puede generar cambios en la recepción de los correos electrónicos.



CSIRT

Equipo de Respuesta ante Incidentes
de Seguridad Informática