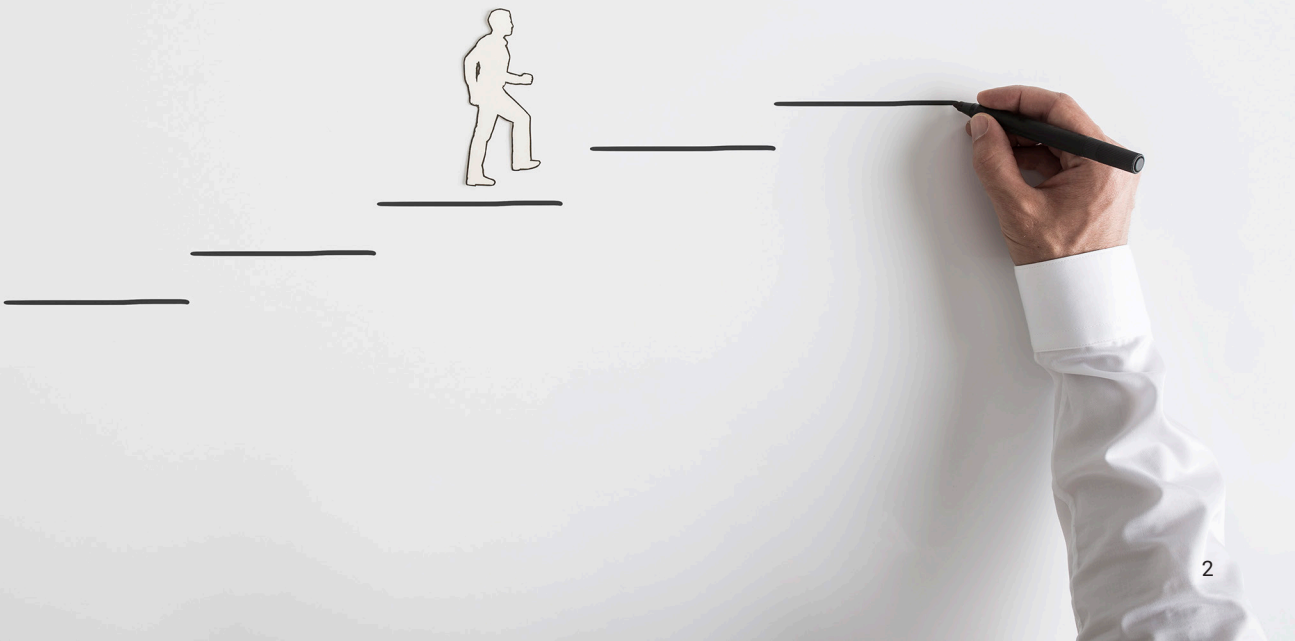
sothis

GESTIÓN SEGURA E INTEGRAL DEL CORREO CORPORATIVO: PROTECCIÓN Y CUMPLIMIENTO

www.sothis.com

Índice



El **correo electrónico** fue una de las primeras herramientas de red que se popularizaron y extendieron en todas las capas de uso y usuarios digitales. La gratuidad o el coste ajustado del mismo, la simplicidad de uso y el factor determinante de digitalizar un medio de comunicación tan eficaz y extendido como era el correo ordinario para convertirlo en instantáneo, añadiéndole, además, funciones nuevas que ampliaban su utilidad, hizo que la adhesión a la herramienta encontrara muy poca de la temida resistencia al cambio, tanto entre particulares como en las organizaciones. En poco tiempo, se convirtió en el medio de comunicación particular y corporativo más potente y extendido.

En un entorno en el que el desarrollo de la tecnología condiciona la duración del uso de las herramientas, el paso de los años y la aparición de nuevos medios de comunicación creados desde y para el entorno digital, medios de comunicación nativos, no solo no han quitado potencia y extensión al correo electrónico como medio de comunicación corporativo, sino que han afianzado su uso y han permitido añadirle nuevas funcionalidades que lo han convertido en una herramienta multifuncional imprescindible para las organizaciones.

> *El correo electrónico corporativo constituye en la actualidad la base de la comunicación interna y externa, con clientes y proveedores, y su utilización se extiende habitualmente a todos los miembros de la organización.*

Sin embargo, pese a su importancia y la progresiva percepción de la misma, **la gestión integral del correo electrónico corporativo es una asignatura pendiente** para muchas organizaciones.

> *La gestión integral y segura del correo electrónico de las organizaciones pasa tanto por garantizar su protección frente a las diferentes formas de ciberdelincuencia como por el cumplimiento normativo y el tratamiento de datos.*

Supone **definir la política corporativa de uso seguro y correcto**, difundirla entre todos los miembros de la organización y garantizar su cumplimento, consiguiendo así actuar en dos frentes críticos como son la seguridad y el cumplimiento, para:

- **Protegerlo frente a las ciberamenazas** y establecer un sistema de detección y neutralización de riesgos.
- **Asegurar en todo momento el cumplimiento normativo** en el tratamiento y la protección de datos en todas y cada una de las acciones de comunicación a través del correo electrónico corporativo llevadas a cabo por cualquier miembro de la organización.

En este dossier, analizaremos el modelo de gestión segura del correo electrónico corporativo, examinando las principales amenazas que ponen en riesgo la seguridad del correo electrónico, la estrategia para combatirlas y, también, las obligaciones derivadas del cumplimiento de la normativa sobre datos que afecta al correo electrónico corporativo.

Protección del correo electrónico corporativo: amenazas y defensa

El correo electrónico corporativo es un punto vulnerable para la seguridad de las organizaciones y se ha convertido en uno de los principales vectores de entrada elegidos por la ciberdelincuencia. La importancia de la herramienta para el buen funcionamiento de la actividad de las organizaciones y el hecho de que su radio de acción incluya a todos los niveles de una organización lo convierten en objetivo y oportunidad para los ciberdelincuentes.

> *Según datos del Informe Ciberamenazas y Tendencias 2019 del CCN-CERT, el correo electrónico estuvo involucrado en más del 90% de los ciberataques.*

A medida que las soluciones tradicionales de seguridad han ido haciendo frente a los ciberataques, **las amenazas se han ido sofisticando** para conseguir burlarlas, hasta convertirlas en insuficientes.

El eslabón más débil de la cadena de seguridad del correo electrónico es el factor humano, y las **técnicas de ingeniería social** desarrolladas por la ciberdelincuencia explotan esta vulnerabilidad. Por eso, **es importante establecer una estrategia de protección multicapa** que no solo contenga defensas basadas en puerta de enlace sino que contemple, también, defensas para neutralizar ataques de ingeniería social con técnicas de puerta trasera.

2.1. Principales amenazas de seguridad asociadas al correo electrónico:

Las amenazas de seguridad asociadas al correo electrónico abarcan **diferentes niveles de gravedad**, que dependen de la particularidad específica de cada ataque:

- La sofisticación de la técnica empleada por el ciberdelincuente: no es lo mismo el *spam* que el *phishing*, por ejemplo, ni en dificultad para llevarlo a cabo ni en probabilidad de éxito. Además, es frecuente encontrar que en un solo ataque se combinan varias técnicas diferentes.

- El tamaño de la organización objeto del ataque: las grandes organizaciones son objetivos muy codiciados por la ciberdelincuencia, sin embargo, sus sistemas de seguridad son mucho más sofisticados y eficaces que los de las pequeñas y medianas empresas, por lo que muchas veces, el ciberataque se dirige simultáneamente a muchas de estas últimas, más vulnerables, que a una sola de las grandes, resultando, así, más fácil conseguir el éxito del ataque.

- El objetivo del ataque: en un mundo en donde la información es poder, no siempre el fraude financiero es el objetivo directo de un ciberataque.

Sean cuales sean las características específicas de cada amenaza de seguridad asociada al correo electrónico corporativo, lo que es común en todos los casos es **su capacidad para comprometer el correcto funcionamiento de la organización** en caso de materializarse.

Las principales amenazas de seguridad asociadas hoy al correo electrónico corporativo son:

Correo no solicitado: Conocido también con los nombres de correo no deseado, *spam* o correo basura, es aquel enviado de forma masiva a destinatarios que no han autorizado dicha comunicación. Aunque comenzó siendo una herramienta barata y simple de marketing, el *spam* es ahora una técnica utilizada por la ciberdelincuencia para acceder a un gran número de objetivos, y suele presentarse combinada con otras técnicas más sofisticadas, ya que sirve para distribuir *malware* o realizar suplantaciones de identidad. Entre todos los destinatarios, solo unos cuantos responderán al envío, pero al afectar a millones de direcciones de correo, el objetivo se cubre. Las direcciones para el envío masivo se recopilan a través de ataques previos a un gran número de libretas o se compran de forma ilegal. En la actualidad, muchos de los envíos masivos se realizan a través de *botnets*, equipos de usuarios o servidores de empresas infectados que reciben comandos de un servidor externo y los ejecutan, dificultando así el rastreo del ciberdelincuente.

Aunque volumen global de correo no solicitado ha ido decreciendo a nivel mundial desde el año 2014, esta disminución tiene mucho que ver con su poca efectividad como herramienta de marketing.

En 2019, el spam representó el 55% del tráfico de correo electrónico mundial, frente al 62% que representaba en 2012 y se observó un aumento en el número de envíos al sector corporativo.

1

El correo no solicitado produce pérdidas de 20 000 millones de USD anuales a las organizaciones, reduce la productividad y afecta al tráfico del servidor.

***Malware*:** A través del correo electrónico, los ciberdelincuentes introducen, por medio de enlaces o documentos adjuntos, alguna forma de descarga de *software* malicioso, conocido como *malware*, en el equipo del receptor, que se infecta, pudiendo convertirse, además, en vector de entrada de *malware* que infecte otros equipos y sistemas. Dentro del concepto de *malware* se agrupan diferentes tipos de programas maliciosos diseñados para inutilizar equipos y redes, controlarlos o extender la infección a otros equipos y redes con el objetivo de generar un beneficio ilegal al ciberdelincuente, como son los virus, los troyanos, los gusanos o el *ransomware*, entre otros.

En 2019, el correo electrónico fue el vector de distribución de *malware* en el 92,45% de los ataques.

2

El *malware* paraliza la actividad de la organización, provocando costes por pérdida de productividad, por pago de rescates para recuperar la operatividad del sistema y por pérdidas financieras por inactividad.

Filtración de datos: Es un incidente que traspasa la información sensible y confidencial de una empresa a un equipo o persona ajenas a la misma. Puede ocurrir de forma accidental o involuntaria, pero también intencionadamente de forma manual o a través de un proceso automatizado a distancia, con la ayuda de *malware*.

La filtración de datos compromete la actividad y la reputación de la empresa en diferentes planos: frente a sus clientes y proveedores, frente a la competencia y también internamente. Suele realizarse a través del correo electrónico, utilizando técnicas de ingeniería social, que consiguen, gracias al engaño, que el usuario ceda sus propios datos o los de la organización en la que trabaja, o a través de técnicas de *malware*. Sin el sistema de protección adecuado, una organización puede sufrir el robo de datos e información sensible sin ser consciente de ello hasta que se materializan las consecuencias.

3

Suplantación: La suplantación de una identidad a través del correo electrónico es uno de los métodos de ingeniería social más utilizados en la actualidad, el ciberataque se lleva a cabo a través de la simulación de una identidad, tan parecida a la real, que la víctima confía en el mensaje y sigue las instrucciones de forma automática sin sospechar nada. Cuando la suplantación afecta a direcciones de remitente, estamos ante la técnica de ingeniería social denominada *e-mail spoofing*.

Según cuál sea la identidad suplantada, la suplantación puede ser:

- Suplantación de dominio, URL y sitio web: se compra un dominio muy parecido a uno legítimo —utilizando técnicas como el *typosquatting*, quitando o añadiendo una letra— o se cambia el dominio de nivel superior, o se crea una URL muy parecida a la legítima que conducen a un sitio web falso idéntico al legítimo en el que se pide introducir información, datos o contraseñas con el señuelo de solucionar o evitar algún problema, o pinchar en algún enlace o documento que descarga *malware*.

- Suplantación de identidad personalizada: los ciberdelincuentes estudian antes a su objetivo y su entorno para recabar datos sobre compañeros, jefes o sitios de confianza y así diseñar un correo con una apariencia y un mensaje que no despierten dudas en el objetivo, pero introduzcan una presión de urgencia, necesidad u oportunidad que exija una actuación rápida, para que no haya tiempo de análisis, y así robar sus datos, conseguir transferencias financieras, contraseñas de acceso a otros sistemas, infectar con *malware* la red corporativa...

  En el informe Tendencias de Seguridad en el Correo Electrónico 2019 de la firma Barracuda se destaca que el 43% de las firmas consultadas habían sido objeto de un ataque de suplantación de identidad personalizada durante ese año.

- Suplantación de identidad lateral: no se produce la falsificación de ningún perfil o sitio web, sino que el ataque se lleva a cabo desde una cuenta de correo que ha sido robada, de tal forma

4

que la cuenta es la legítima, pero está controlada por el ciberdelincuente, que se hace pasar por su dueño real para engañar al receptor y conseguir que le entregue información, siga los pasos para infectar su equipo con *malware* o realice una acción determinada, generalmente financiera.

- Suplantación de marcas: el ataque se hace a través de una comunicación que aparenta ser la de una marca muy reconocida con la que el objetivo tiene o ha tenido alguna relación. El correo incluye un mensaje diseñado para que el objetivo desvele sus claves, datos de la tarjeta de crédito o información que identifica al usuario, como número de DNI, tarjeta de la SS...

4

Microsoft es la marca objeto de un mayor número de suplantaciones a nivel mundial, ya que sus credenciales tienen un gran valor para la ciberdelincuencia, porque permiten acceder a los sistemas de las organizaciones.

Usurpación de cuentas: El ciberdelincuente toma el control de una cuenta de correo electrónico corporativo y de esta forma tiene acceso a conversaciones confidenciales entre miembros de la organización que le proporcionan información y datos sensibles que luego utiliza para llevar a cabo otros ataques e, incluso, realizar chantaje a la organización para evitar que dicha información se haga pública. También, el robo de una cuenta de correo electrónico corporativo se utiliza para llevar a cabo ataques como el fraude del CEO, un tipo específico de suplantación de identidad lateral: se envía un mensaje, normalmente sin archivos adjuntos o enlaces, a un empleado desde la cuenta comprometida de un alto cargo para que realice con urgencia traspasos u otras acciones financieras en favor del ciberdelincuente.

5

2.2. Defensa del correo electrónico frente a las amenazas.

Para defender con eficacia el correo electrónico corporativo de estas amenazas, se necesita una actuación combinada de tecnología y personas:

✓ **Tecnología:** La protección integral del correo electrónico corporativo a través de soluciones de tecnología requiere una **estrategia multicapa**, porque las soluciones tradicionales, si bien siguen siendo efectivas, no son suficientes para abarcar todos los riesgos en el entorno actual de amenazas más evolucionadas y sofisticadas.

- Las **soluciones tradicionales de seguridad basadas en la puerta de enlace** funcionan filtrando los mensajes de entrada y salida del correo electrónico para detectar contenido malicioso. Estas soluciones crean un perímetro de seguridad basado en filtros alrededor del correo electrónico, gracias a los cuales identifican IP de reputación débil, indicios de contenido malicioso en los mensajes, el correo no solicitado, *malware* y URL de redacción dudosa. Las puertas de enlace son imprescindibles en la detección y neutralización del correo no solicitado, la extracción de datos, el *malware* y los ataques de día cero, y **constituyen la**

capa base de la seguridad del correo electrónico, siendo, sin embargo, poco útiles ante las técnicas más modernas de ingeniería social, ya que su funcionamiento, basado en filtros, es poco eficaz a la hora de detectarlas.

- Las **soluciones de defensa de la bandeja de entrada** del correo electrónico constituyen la otra capa de seguridad que completa a las puertas de enlace. Esta solución de seguridad se basa en API para integrarse directamente en el entorno del correo electrónico, incluidas las bandejas de entradas individuales. Esto la habilita para recabar datos sobre los modos de comunicación de cada persona integrante de la organización y establecer patrones individualizados a través de programas de AI, con los que se crea un gráfico de identidad propio de cada usuario y que comprende datos como el lugar desde el que habitualmente inicia la sesión cada empleado, sus destinatarios y remitentes habituales, sus comunicaciones más repetidas... Este gráfico sirve después para detectar y alertar sobre cualquier comportamiento anómalo o acción de comunicación no habitual en los correos remitidos y recibidos en dicha cuenta.

  Las soluciones de defensa de la bandeja de entrada basadas en API son efectivas en la detección y neutralización de ataques basados en ingeniería social, como los diferentes tipos de suplantación o el robo de cuentas, y **constituyen la capa de protección avanzada** del correo electrónico corporativo.

✓ **Profesionales especializados en soluciones de seguridad:** La complejidad y sofisticación de las amenazas y los ataques exigen que las tareas de elaboración de estrategias, actualización de defensas, análisis de riesgos, y protección avanzada de la seguridad del correo electrónico corporativo, que incluye la detección, monitorización y neutralización de los incidentes, deban ser dirigidas, realizadas y supervisadas por equipos de profesionales especializados en seguridad digital y del correo electrónico, para que resulten eficaces. Además, la formación continua de las personas de la organización en el uso seguro del correo electrónico, el conocimiento actualizado de las nuevas amenazas y las medidas de protección frente a las técnicas de ingeniería social ha de ser realizada por el mismo equipo de profesionales especializados.

✓ **Personas de la organización:** Los usuarios del correo electrónico corporativo, afectando a cualquier jerarquía del organigrama de la organización, son el eslabón más débil de la cadena de seguridad y el objetivo de las técnicas de ingeniería social. A través de la formación continuada y actualizada, deben tomar conciencia de las amenazas más comunes, las de creación reciente y las técnicas para neutralizarlas, así como de la necesidad de llevar a cabo medidas de protección de forma rutinaria, como no pinchar en enlaces dudosos, no descargar archivos adjuntos sin hacer una comprobación previa del remitente, no proporcionar claves ni contraseñas, confirmar por otra vía las peticiones de movimientos financieros, incluso aunque provengan de cuentas fiables de la organización o implementar las verificaciones en dos paso, entre otras.

El correo electrónico y la protección de datos: cumplimiento del RGPD

Una vez diseñada la vertiente de la protección en la gestión del correo electrónico corporativo, queda la otra vertiente, la del **cumplimiento de la normativa sobre tratamiento y protección de datos** que afecta al correo electrónico corporativo igual que a cualquier herramienta de las organizaciones que maneje datos e información de terceros.

> *Un correo electrónico corporativo no estará gestionado con eficacia si en algunas actuaciones incumple las obligaciones impuestas por el RGPD, ya que podría ser motivo de sanciones administrativas, demandas particulares y crisis de reputación.*

EL RGPD obliga a la **protección de datos por diseño y por defecto**, por lo que las organizaciones deberán cumplir esta obligación en cada uno de los productos o servicios existentes o nuevos que ofrezca y en todos los medios de comunicación con terceros que utilice. Además, el RGPD establece el principio de «minimización de datos», solo permitiendo que se recaben aquellos necesarios en relación con los fines para los que son tratados.

Entre las **obligaciones sobre protección de datos** que establece el RGPD que afectan al correo electrónico corporativo están:

- **Campañas de email marketing:** se precisa **consentimiento expreso del destinatario para recibir la comunicación**, a la vez que hay que darle el poder de revocar dicho consentimiento en cualquier momento. Este consentimiento ha de ser informado, recabarse en un lenguaje claro y las solicitudes de consentimiento han de ser distinguibles claramente de otros asuntos. El espíritu de la ley no deja lugar a los consentimientos recabados sin transparencia.

  Puede establecerse comunicación sin consentimiento expreso siempre y cuando haya mediado una relación contractual o de prestación de servicios entre el remitente y el receptor, y siempre referida a dicha relación.

- **Información sobre el tratamiento de datos:** si en los correos se van a recopilar datos personales, **el receptor ha de estar informado** sobre el tipo de datos, la política de protección de datos de la organización, además del motivo por el que esos datos van a recopilarse y cómo se van a utilizar o almacenar. Informar sobre el tratamiento de datos no tiene que ver ni se solventa con la cláusula de confidencialidad que se incluye normalmente en los correos electrónicos corporativos. La información sobre el tratamiento de datos exige que la organización tenga diseñada y redactada una política de protección de datos, que recoja las particularidades de su actividad.

- **Protección de los datos de terceros:** deben contemplarse para los datos personales obtenidos a través del correo electrónico corporativo las mismas **medidas de seguridad** que la

organización toma para proteger su información confidencial. Técnicas como el cifrado del correo electrónico sirven para garantizar, además, la confidencialidad de las comunicaciones. Cada organización deberá estudiar sus puntos vulnerables en cuanto a seguridad de los datos de terceros y establecer la estrategia de seguridad más eficaz para protegerlos.

- ✓ **Almacenamiento y borrado de los datos de terceros:** los datos han de **almacenarse de forma segura**, pero, además, han de ser **borrados** una vez que la finalidad para la que hayan sido recabados haya terminado o haya transcurrido el tiempo marcado por la ley, limitación del plazo de conservación, o por la política de protección de datos de la propia organización.

La regulación exige, por tanto, que las organizaciones tengan establecida una **política de extracción y protección de datos de terceros** en la que se equilibren con precisión los intereses comerciales legítimos de las mismas con el derecho de los terceros sobre sus datos personales. En caso de conflicto, son las organizaciones las que tienen la carga de demostrar que el tratamiento de los datos de terceros es suficiente y ajustado a la ley.

Servicios gestionados de correo seguro de Sothis

La gestión segura e integral del correo electrónico corporativo es una necesidad de las organizaciones. Garantiza la seguridad de uno de los principales vectores de entrada de los ciberdelincuentes, como es el correo electrónico corporativo, y el cumplimiento legal sobre el tratamiento de los datos de terceros contenidos en el mismo.

Desde **Sothis**, ayudamos a las organizaciones con nuestros **servicios gestionados de correo seguro**, desde nuestro SOC certificado 27001 y ENS. Contamos con un portfolio completo de servicios para mejorar la seguridad de las comunicaciones de correo electrónico, detectar posibles ataques y amenazas para protegerlas ante ataques y guiar a la organización en la forma de conseguir que las normas legales se cumplan.

¡Gracias!