REDIRECCIÓN DEL CORREO ELECTRÓNICO DE EDUCAMADRID A CUENTAS DE CORREO AJENAS A LA COMUNIDAD DE MADRID

Esta Delegación ha tenido conocimiento a través de diversas consultas de los interesados de que es práctica habitual que personas que disponen de una cuenta de correo institucional de EducaMadrid las configuren para redirigir todos los mensajes entrantes a cuentas de correo particulares ajenas a la Comunidad de Madrid.

El correo corporativo es una herramienta que las empresas y organizaciones ponen a disposición de sus empleados con el fin de tener el control de su información confidencial. Los centros deben entender que cuando nos relacionamos profesionalmente no podemos utilizar nuestras cuentas personales, y mucho menos en situaciones excepcionales, como las de teletrabajo con motivo la pandemia COVID-19, donde los empleados utilizan sus propios dispositivos.

El Centro Criptológico Nacional, en sus Guías de la Serie CCN-STIC-800 establece las políticas y procedimientos adecuados para la implementación de las medidas contempladas en el Esquema Nacional de Seguridad (RD 3/2010)[1]. La Guía de seguridad de las tic (ccn-stic-814). seguridad en correo electrónico, recoge la siguiente consideración:

> ***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.***

Según el art. 36.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, "*cuando el delegado de protección de datos aprecie la existencia de una vulneración relevante en materia de protección de datos lo documentará y lo comunicará inmediatamente a los órganos de administración y dirección del responsable o el encargado del tratamiento*".

En consecuencia, esta Delegación **instó a las Direcciones de Area Territorial que comunicasen a los centros educativos,** para que estos a su vez lo pongan en conocimiento de los interesados, que toda persona usuaria de cuentas de correo de EducaMadrid deberá abstenerse de activar la redirección de sus mensajes a cuentas de correo particulares ajenas a la Comunidad de Madrid, y que además deberá eliminar las redirecciones existentes con carácter inmediato. Deberá informarse, además, a los interesados, que en caso de emplear tal recurso serán inmediatamente responsables directos de las consecuencias que dicha acción puedan acarrear.

Incluimos, a título informativo, las consideraciones del Centro Criptológico Nacional a este respecto.

Madrid Digital también recomienda estas buenas prácticas en materia de ciberseguridad en su Boletín informativo. En el dominio podemos sustituir la palabra "salud" por "educa".

LA DELEGACIÓN DE PROTECCIÓN DE DATOS

2021

[1] Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Anexo I – El Centro Criptológico Nacional y el uso del correo electrónico en las organizaciones

El Centro Criptológico Nacional (CCN) en su Guía de implantación del Esquema Nacional de Seguridad, de obligado cumplimiento para todas las Administraciones públicas y empresas que les prestan servicios, señala la limitación del uso del correo electrónico al estrictamente profesional y concienciación y formación relativas al uso adecuado del mismo, para salvaguardar la seguridad de la información.

Así, en su GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-814). SEGURIDAD EN CORREO ELECTRÓNICO, señala que Las organizaciones deben regular formalmente, entre otros, el uso del correo electrónico corporativo por parte de sus empleados, establecer medidas disciplinarias a que haya lugar en caso de incumplimientos de los deberes y obligaciones en el uso del correo electrónico y la **restricción en el uso de correos personales para envío de información sensible**.

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**.

Particularmente importante es el apartado 4.2. de esta guía, cuyo contenido recomendamos para elaborar la resolución que se dicte al respecto:

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.