

Notas de la plantilla

- Esta plantilla está diseñada para proporcionar contenido de muestra para un documento sobre la política de seguridad de la información y describe los riesgos de los medios sociales, la política de empresa, la educación de los empleados y los controles técnicos.
- Esta plantilla está destinada a servir únicamente como ejemplo o referencia y no representa asesoría legal. Para éste tipo de asesoría, consulte su abogado.
- Cualquier parte de esta plantilla puede ser modificada, los elementos resaltados indican las áreas donde se requiere una personalización.
- Una versión personalizada de este documento o parte de éste pueden ser incorporados en el uso aceptable de Internet o en documentos de políticas de seguridad.
- El contenido de este documento puede ser copiado y pegado en sus propios archivos, o puede quitar la marca de agua de fondo y basarse en el diseño del documento / propiedades de fondo.

Política de Uso Aceptable para Medios Sociales

Información general

[Inserte el nombre de la compañía] reconoce que hay razones de negocios [y personales?] legítimas para el uso de los medios sociales en el trabajo o el uso de recursos informáticos corporativos. Para permitir que los empleados aprovechen el valor empresarial de estos sitios y para promover un lugar de trabajo abierto, confiable y colaborativo, la política de [Inserte el Nombre de la empresa] permite a [designados o todos?] empleados a utilizar los medios sociales dentro de las directrices que se especifican a continuación.

¿Qué son los Medios Sociales?

Dentro de la categoría de los medios sociales se incluye cualquier sitio Web en el que los visitantes puedan publicar información para un grupo de visitantes. La información compartida puede incluir (pero no se limita a) datos personales, opiniones, investigaciones, comentarios o información comercial. Ejemplos de estos sitios web incluyen entidades reconocidas como tales como Facebook, Twitter, YouTube y LinkedIn. Sin embargo, los blogs, los foros de interés especial, las comunidades de usuarios también se consideran medios sociales.

Autorización de Medios Sociales

Uso General de Los Medios Sociales

El uso general de sitios de medios sociales es permitido para los siguientes empleados [Inserte, Empleados, Títulos, Grupos de, "Todos los empleados"].

Contenido Corporativo en los Medios Sociales

La publicación de contenido empresarial en medios sociales (por ejemplo, la página corporativa de Facebook) está permitida sólo a los siguientes empleados autorizados para representar de forma pública a la empresa: [Insertar, empleados, títulos, grupos].

Política Sobre el Contenido Inapropiado

En los medios sociales se encuentra contenido personal y de negocios legítimos, también se encuentra contenido que no es apropiado para el lugar de trabajo incluyendo nudismo, violencia, abuso de drogas, sexo y juegos de azar. Por lo tanto, la misma política de contenido inapropiado que se aplica al uso de la Web, también se aplica al contenido que se encuentra dentro de los medios sociales. Los empleados no deben tener acceso a contenidos inapropiados mientras estén en el trabajo o durante el uso de recursos de la empresa. Una lista completa de las categorías de contenido consideradas inapropiadas se pueden encontrar en Plantilla para la Política de Uso Aceptable de Internet (nota: una plantilla de éste documento es proporcionada en ésta guía). Asimismo, los empleados deben usar el sentido común y consideración por los demás a la hora de decidir qué contenido es apropiado para el lugar de trabajo.

La compañía cuenta con los controles técnicos para proporcionar recordatorios, auditorías y hacer cumplir esta política (ver **Controles Técnicos** más abajo.)

Política de Productividad

[Inserte el nombre de la compañía] reconoce que los empleados tienen la necesidad, en ocasiones, de atender asuntos personales dentro de los medios sociales, mientras que están en el trabajo o mientras usan recursos de la empresa. Por lo tanto, [Inserte el nombre de la empresa] permite un acceso limitado a los contenidos no profesionales de los medios sociales. Por ejemplo, los empleados tienen acceso a las aplicaciones de comunicación personal, correo electrónico y al contenido de los blogs en los medios sociales por un período de hasta [Insertar cuota de tiempo] por día. Es responsabilidad del empleado asegurarse que los asuntos personales no afecten la calidad o productividad de su trabajo. Esta política es coherente con la política de productividad–definida para la Web en general , fuera de los medios sociales –de [Inserte el Nombre de la empresa]. Una lista completa de categorías de contenido considerado inapropiado se puede encontrar en Plantilla para la Política de Uso Aceptable de Internet (nota: una plantilla de éste documento es proporcionada en ésta guía).

La compañía cuenta con los controles técnicos para proporcionar recordatorios, auditorías y hacer cumplir esta política (ver **Controles Técnicos** más abajo.)

Política para la Publicación de Contenido y Confidencialidad

Las siguientes son las directrices de la política con respecto a lo que se debe y no se debe hacer cuando se va a publicar un contenido en los medios sociales. Estas directrices se aplican a todos los medios sociales ya sean personales o comerciales. Los empleados son responsables por el contenido que publican en los medios de comunicación social y pueden ser individualmente responsables por el contenido publicado. Los empleados también pueden ser objeto de medidas disciplinarias por parte de [Nombre de la

[empresa] causadas por la publicación de contenido inapropiado o confidencial. Estas directrices cubren solamente una parte de todos los escenarios posibles de publicación de contenido y no sustituyen el buen juicio.

- Conozca y siga todas las directrices de privacidad y confidencialidad contenidas en el Manual del Empleado de [Nombre de la empresa]. Todas las pautas del manual, incluidas leyes tales como los derechos de autor, el uso justo y las leyes de divulgación de información financiera se aplican a los medios sociales.
- No revele o utilice información confidencial o reservada de [Inserte el Nombre de la empresa], o de cualquier otra persona o empresa. Por ejemplo, pida permiso antes de publicar una foto de alguien en una red social o publicar en un blog una conversación de carácter privado.
- No haga comentarios acerca del precio de las acciones de [Nombre de la empresa] o acerca de su información financiera confidencial, como el rendimiento futuro del negocio o planes de negocios.
- NO cite o use la referencia de clientes, socios o proveedores sin su consentimiento por escrito.
- IDENTIFIQUESE. Algunas personas trabajan de forma anónima, utilizando seudónimos o nombres falsos. [Inserte el Nombre de la empresa] se opone a ésta práctica.
- Sea profesional. Si usted se ha identificado como empleado de [Nombre de la empresa] dentro de un sitio web social donde está conectado con sus colegas, directivos e incluso con los clientes de [Inserte el Nombre de la empresa]. Asegúrese de que el contenido asociado a usted es consistente con su trabajo en [Nombre de la empresa].
- Pida autorización – para publicar o informar sobre las conversaciones de carácter privado o interno de [Inserte el Nombre de la empresa] y en caso de duda siempre pida asesoría al departamento legal de [Nombre de la empresa].
- Hable en primera persona al participar personalmente en medios de comunicación social. Deje claro que usted está hablando por sí mismo y no en nombre de [Nombre de la empresa].
- Use un descargo de responsabilidad *DISCLAIMER* – Si publica individualmente en medios de comunicación de [Nombre de la empresa] y tiene algo que ver con su trabajo o con temas relacionados con [Inserte el Nombre de la empresa], use un aviso como éste: "Los mensajes de este sitio son míos y no necesariamente son representación de [Nombre de la empresa]."
- Haga un enlace con la fuente – Cuando haga una referencia para un cliente, socio o proveedor, si es posible relaciónelo con la fuente.
- Sea consciente de su asociación con los medios sociales de [Inserte el Nombre de la empresa] – Si usted se identifica como empleado de [Inserte Nombre de la empresa], asegúrese de que su perfil y el contenido relacionado sea consistente con la forma en que desea presentarse a sus colegas y clientes.

- Use su buen juicio – Recuerde que lo que publica siempre trae consecuencias. Si usted está a punto de publicar algo que lo incomoda, incluso en lo más mínimo, revise las sugerencias anteriores y piense en el por qué de las mismas. Si usted todavía no está seguro, y lo que va a publicar está relacionado con asuntos de **[Inserte Nombre de la empresa]**, no dude en hablar con su gerente o simplemente no lo publique. Usted tiene la responsabilidad exclusiva de lo que publique en su blog o en cualquier forma de medio social.
- NO utilice insultos étnicos, insultos personales, obscenidades, ni aborde ninguna conducta que no sea aceptable en el lugar de trabajo de **[Nombre de la empresa]**. Además, usted debe mostrar la debida consideración hacia la privacidad de los demás y hacia los temas que pueden considerarse inaceptables o irritantes.
- NO lleve a cabo negocios confidenciales con un cliente o socio a través de su página personal en un medio social u otros.
- No registre cuentas con la marca de **[Inserte el Nombre de la empresa]** o cualquier otra marca registrada o no registrada.

[Inserte el Nombre de la empresa] emplea controles técnicos para proporcionar recordatorios, supervisar y cumplir estas reglas (vea **Controles Técnicos** más abajo).

Prevención de Malware y Crimen Online

Los medios sociales son comúnmente utilizados por la comunidad criminal online para ofrecer malware y llevar a cabo acciones destinadas a daños a la propiedad o robo de información confidencial. Para minimizar los riesgos relacionados con éstas amenazas, adhiérase a los siguientes lineamientos. Aunque éstos le ayudarán a reducir el riesgo, no cubren todas las posibles amenazas y no son un sustituto del buen juicio.

- No utilice la misma contraseña que utiliza para acceder a recursos de computación de la empresa, para acceder a medios sociales.
- No siga enlaces en páginas de medios sociales que hayan sido puestos por personas u organizaciones que usted no conozca.
- No descargue software publicado o recomendado por personas u organizaciones que no conozca.
- Use una aplicación de seguridad, como Defensio (www.defensio.com), para proteger las páginas de medios sociales personales y de la empresa.
- Si algún contenido que usted encuentre en alguna página web de medios sociales le parece sospechoso de alguna manera, cierre el navegador y no regrese a esa página.
- Configure las cuentas de los medios sociales para cifrar las comunicaciones siempre que sea posible. Facebook, Twitter y otros tienen el soporte de cifrado como una opción. Esto es extremadamente importante para los usuarios que se conectan a través de puntos de acceso Wi-Fi.

[Inserte el Nombre de la empresa] emplea controles técnicos para proporcionar recordatorios, auditorías y cumplir estas reglas.

Educación Para Empleados

Un documento de educación para empleados comunicando los riesgos en los medios sociales, la política de [Inserte el Nombre de la empresa] y las directrices para mitigar el riesgo debe añadirse al manual de los empleados y presentarse durante el entrenamiento de nuevos empleados. Todos los empleados deben ser notificados acerca de éste documento desde su creación y cuando sea modificado.

Controles Técnicos

La política de [Insertar Nombre de la empresa] para el uso aceptable de medios sociales descrita anteriormente es supervisada y aplicada por un sistema Secure Web Gateway. El Secure Web Gateway inspecciona comunicaciones vía Web entrantes y salientes de los empleados para hacer cumplir la política de uso aceptable, evitar la pérdida de información confidencial y bloquear ataques Web (malware, phishing, etc.) El Secure Web Gateway puede ser desplegado en las instalaciones, como un Security-as-a-Service (SaaS), o como un sistema híbrido de on-premise/SaaS. El Secure Web Gateway debe asegurar todos los computadores que sean propiedad de la empresa y para uso de los empleados, incluyendo los móviles como ordenadores portátiles con conexiones directas de Internet. El Secure Web Gateway debe incluir las siguientes funciones.

- **Política del Contenido de Medios Sociales** – La capacidad de aplicar las políticas de uso aceptable del contenido de todas las páginas de medios sociales y hacerlo a través de todas las categorías de contenidos (por ejemplo, deportes, juegos, adultos). No es suficiente clasificar los medios sociales en el nivel de dominio o URL. La clasificación del contenido de los medios sociales debe ser probada, como mínimo, al visitar una selección (> 25) de páginas populares de medios sociales. Una lista de las páginas populares de Facebook se puede encontrar en <http://statistics.allfacebook.com/pages/leaderboard/>.
- **Clasificación de Riesgo Compuesto**– La capacidad de combinar información de múltiples análisis de seguridad de contenidos para clasificar contenido e identificar ataques en tiempo real. Los analizadores deben incluir bases de datos de URL, reputación, firmas de contenidos, antivirus, y análisis del contenido. La clasificación de riesgo compuesto permite que Secure Web Gateway identifique contenido malicioso, tales como esquemas de phishing en Facebook y cero malware al día en tiempo real.
- **Detección de Información Confidencial o Sensible**– La capacidad para identificar las cadenas de datos confidenciales y la identificación de violaciones por salida de datos confidenciales. Por ejemplo, la solución debe diferenciar entre publicar solo el número de seguridad social de un empleado (no es una violación), y la publicación del número de seguridad social combinado con el nombre del

empleado (violación). Diccionarios de palabras clave y las expresiones regulares no cumplen con este requisito ya que son específicos de cada país o región

- **Identificación de datos contenidos en Base de Datos y Documentos Personalizados**– La capacidad para identificar los registros personalizados contenidos en bases de datos (por ejemplo, registros de los clientes) y documentos (por ejemplo, planes de negocio).