PLAN DE CIBERSEGURIDAD EN LOS PUESTO DE TRABAJO

Icono

Descripción generada automáticamenteDaniel Ubalde

En este documento se van a reflejar las normas de ciberseguridad aplicables a los trabajadores de Bionica Automations en materia de los puestos de trabajo.

Contenido

[1. Políticas descritas 2](#_Toc119859698)

[2. Contraseñas 3](#_Toc119859699)

[2.1. Resumen 3](#_Toc119859700)

[2.2. Propósito 3](#_Toc119859701)

[2.3. Audiencia 3](#_Toc119859702)

[2.4. Detalles de la política 3](#_Toc119859703)

[2.4.1. Contraseñas de usuarios 3](#_Toc119859704)

[2.4.2. Contraseñas de administradores 3](#_Toc119859705)

[2.4.3. Protección de contraseñas 4](#_Toc119859706)

[3. Escritorio limpio 5](#_Toc119859707)

[3.1. Resumen 5](#_Toc119859708)

[3.2. Propósito 5](#_Toc119859709)

[3.3. Detalles de la política 5](#_Toc119859710)

[4. Uso del correo electrónico 6](#_Toc119859711)

[4.1. Resumen 6](#_Toc119859712)

[4.2. Propósito 6](#_Toc119859713)

[4.3. Audiencia 6](#_Toc119859714)

[4.4. Legal 6](#_Toc119859715)

[4.5. Detalles de la política 6](#_Toc119859716)

[4.6. Uso incidental 8](#_Toc119859717)

[4.7. Retención de correos 8](#_Toc119859718)

[4.8. Archivado de correos 8](#_Toc119859719)

[5. Actualizaciones 9](#_Toc119859720)

[5.1. Resumen 9](#_Toc119859721)

[5.2. Propósito 9](#_Toc119859722)

[5.3. Audiencia 9](#_Toc119859723)

[5.4. Detalles de la política 9](#_Toc119859724)

[6. Redes sociales 10](#_Toc119859725)

[6.1. Descripción 10](#_Toc119859726)

[6.2. Detalles de la política 11](#_Toc119859727)

# Políticas descritas

1. Contraseñas
2. Escritorio limpio
3. Uso de correo electrónico
4. Actualizaciones
5. Redes sociales

Referencias y enlaces

<https://sistinfo.uca.es/wp-content/uploads/2018/06/documento_explicativo_bloque_III_el_puesto_de_trabajo-UCA.pdf>

<https://si.ua.es/es/documentos/servicios/seguridad/seguridad-trabajo-informatico.pdf>

<https://resources.workable.com/cyber-security-policy>

<https://purplesec.us/resources/cyber-security-policy-templates/#CleanDesk>

<https://www.csoonline.com/article/3019126/security-policy-samples-templates-and-tools.html>

<https://www.lbmc.com/blog/document-management-policy-development/>

# Contraseñas

## Resumen

Las contraseñas son un aspecto muy importante cuando hablamos de proteger cuentas. Son la primera línea de defensa frente a el acceso no autorizado a las mismas. Desde Bionica Automations nos comprometemos a seleccionar contraseñas seguras para proteger nuestra red corporativa. Tanto empleados como proveedores que tengan acceso a las redes de Bionica Automations son responsables de tomas las medidas necesarias para escoger y securitizar sus contraseñas.

## Propósito

El propósito de esta política es establecer una serie de reglas para la creación de contraseñas seguras, su correcto almacenamiento y cada cuento tiempo deben cambiar.

## Audiencia

Esta política es aplicable a todo el personal de Bionica Automations que posea de una cuenta corporativa o cualquier tipo de acceso que requiera una contraseña para acceder a las instalaciones de Bionica Automations, para el acceso a las redes corporativas de Bionica Automations o gestiona información privada de Bionica Automations.

## Detalles de la política

### Contraseñas de usuarios

Todas las contraseñas de acceso a la red corporativa de Bionica Automations tiene n que cumplir los siguientes requisitos:

* Las contraseñas deben cambiar cada 90 días
* Las contraseñas deben tener un mínimo de 10 caracteres
* Las contraseñas deben contener una combinación de caracteres alfanuméricos y caracteres especiales cuando el sistema informático lo permita (!@#$%^&\*\_+=?/~’;’,<>|\).
* Las contraseñas no pueden estar relacionadas con la persona que las crea como puede ser el nombre de usuario, el número de la seguridad social, el DNI, un apodo, el cumpleaños, etc.
* Las contraseñas no pueden ser palabras del diccionario o acrónimos
* Las contraseñas no se pueden reutilizar en 1 año

### Contraseñas de administradores

Todas las contraseñas de administradores tienen que seguir las siguientes reglas:

* La contraseña debe cambiar cada 6 meses
* La contraseña debe tener un mínimo de 12 caracteres y contener a menos tres de los siguientes tipos de caracteres: mayúsculas, minúsculas, números, caracteres especiales.
* Si hay contraseñas que nunca expiran deben estar documentadas y seguir los requisitos mencionados en el punto anterior
* Los administradores no pueden eludir la política de contraseñas en aras de la facilidad de uso

### Protección de contraseñas

* No se debe usar la misma contraseña para múltiples cuentas.
* Nunca se deben compartir las contraseñas con nadie. Todas las contraseñas están catalogadas como información confidencial de Bionica Automations.
* Las contraseñas guardadas deben ser encriptadas
* Las contraseñas un deben ser escritas en correos electrónicos ni en otras formas de comunicación electrónica
* Las contraseñas nunca deben ser dichas o escritas por teléfono
* Las contraseñas nunca deben ser reveladas en cuestionarios o formularios de seguridad
* Las contraseñas de Bionica Automations nunca deben ser compartidas a nadie, incluso compañeros de trabajo, jefes, miembros de tu familia mientras estás de vacaciones.
* Las contraseñas nunca deben ser escritas en papel y almacenadas en la oficina de la empresa. Las contraseñas no pueden almacenar se en texto plano en dispositivos electrónicos
* Si la seguridad de una cuenta se ve comprometida hay que cambiar su contraseña de inmediato y avisar al soporte IT
* Nunca se debe habilitar (recordar contraseñas o similares) en paginas web ni hardcodear contraseñas en código a excepción de casos puntuales como por ejemplo backups automáticos
* Al abandonar el puesto de trabajo nunca se debe dejar el equipo desbloqueado, además de configurar un salvapantallas con contraseña.
* Cualquier tarjeta física, tokens RSA o método de autenticación deberá ser devuelto al terminar la relación laboral con Bionica Automations.

# Escritorio limpio

## Resumen

Bionica Automations se compromete a proteger la privacidad de sus empleados y miembros y también protegerá la confidencialidad de la información no pública de conformidad con las leyes estatales y federales.

Bionica Automations tiene la obligación de garantizar la seguridad y confidencialidad de los datos de miembros y de proteger estos datos contra el acceso no autorizado que podría resultar en cualquier tipo de pérdida o inconveniente para sus miembros.

## Propósito

El propósito y el principio de una política de "escritorio limpio" es garantizar que los datos confidenciales no estén expuestos a personas que puedan pasar por el área, como miembros, personal de servicio y ladrones. Fomenta la gestión metódica del espacio de trabajo.

Debido al riesgo de verse comprometida, la información confidencial siempre debe tratarse con cuidado.

## Detalles de la política

Para mantener la seguridad y privacidad de la información personal de los empleados y miembros de Bionica Automations deben observar la regla de "escritorio limpio". Todos los empleados deben tomar las medidas apropiadas para evitar que personas no autorizadas tengan acceso a la información, las aplicaciones o los datos de los miembros. Los empleados también deben hacer una verificación concienzuda de su entorno de trabajo circundante para garantizar que no haya pérdida de confidencialidad en los medios de datos o documentos.

La política de escritorio limpio se aplica a:

* Planificadores de trabajo que puedan contener información confidencial
* Archivadores, armarios de almacenamiento y maletines que contienen información sensible o confidencial
* Cualquier dato confidencial o sensible, incluidos informes, listas o declaraciones. Los datos sensibles se refieren a la información personal y los datos restringidos. La información personal incluye, pero no se limita a:
  + Nombres individuales
  + Número de la seguridad social
  + Permiso de conducir
  + Número de cuenta
* Aparatos electrónicos, incluidos teléfonos móviles
* Llaves para acceder a información sensible
* Documentos que contengan información sensible
* Documentos en impresoras, fotocopiadoras y faxes
* El ordenador de trabajo y contraseñas
* Medios de almacenamiento externos como USBs, CDs

# Uso del correo electrónico

## Resumen

El correo electrónico de Bionica Automations debe administrarse como un recurso valioso y de misión crítica. Así, esta política se establece para:

* Crear prácticas prudentes y aceptables con respecto al uso de los recursos de información
* Educar a las personas que pueden utilizar los recursos de información con respecto a sus responsabilidades asociadas con dicho uso
* Establezca un cronograma para retener y archivar el correo electrónico

## Propósito

El propósito de esta política es establecer reglas para el uso del correo electrónico de Bionica Automations para enviar, recibir o almacenar correo electrónico.

## Audiencia

Esta política se aplica por igual a todas las personas a las que se otorgan privilegios de acceso a cualquier recurso de información de Bionica Automations con capacidad para enviar, recibir o almacenar correo electrónico.

## Legal

Las personas involucradas pueden ser consideradas responsables de:

* Enviar o reenviar correos electrónicos con comentarios calumniosos, difamatorios, ofensivos, racistas u obscenos.
* Enviar o reenviar información confidencial sin permiso
* Enviar o reenviar material protegido por derechos de autor sin permiso
* Enviar o reenviar a sabiendas un archivo adjunto que contiene un virus

## Detalles de la política

El correo electrónico corporativo no es privado. Los usuarios renuncian expresamente a cualquier derecho de privacidad en cualquier cosa que creen, almacenen, envíen o reciban en los sistemas informáticos de Bionica Automations. Bionica Automations puede, pero no está obligado a, monitorear los correos electrónicos sin notificación previa. Todos los correos electrónicos, archivos y documentos, incluidos los correos electrónicos, archivos y documentos personales, son propiedad de Bionica Automations, pueden estar sujetos a solicitudes de registros abiertos y se puede acceder a ellos de acuerdo con esta política.

El correo electrónico entrante debe tratarse con sumo cuidado debido a los riesgos inherentes a la seguridad de la información. Se utiliza una aplicación antivirus para identificar códigos o archivos maliciosos. Todo el correo electrónico está sujeto al filtrado entrante de archivos adjuntos de correo electrónico para buscar virus, códigos maliciosos o spam. El spam se pondrá en cuarentena para que el usuario lo revise para determinar su relevancia. La introducción de un virus o código malicioso en los sistemas de Bionica Automations podría causar estragos en la capacidad de realizar negocios. Si el escaneo automático detecta un riesgo de seguridad, se debe notificar inmediatamente al departamento de TI.

Se han iniciado prácticas contra la suplantación de identidad para detectar correos electrónicos falsificados. Los empleados deben ser diligentes en la identificación de un correo electrónico falsificado. Si se ha producido una suplantación de identidad por correo electrónico, se debe notificar inmediatamente al departamento de TI.

Los correos electrónicos entrantes se analizan en busca de archivos adjuntos maliciosos. Si se identifica que un archivo adjunto tiene una extensión que se sabe que está asociada con malware, o que es propenso al abuso por parte de malware o malos actores, o que presenta un mayor riesgo, el archivo adjunto se eliminará del correo electrónico antes de la entrega. El rechazo de correo electrónico se logra a través de la lista de dominios y direcciones IP asociadas con actores maliciosos. No se entregará ningún correo electrónico entrante procedente de un actor malicioso conocido. Cualquier cuenta de correo electrónico que se comporte mal al enviar spam se cerrará. Se realizará una revisión de la cuenta para determinar la causa de las acciones.

El correo electrónico debe usarse con fines comerciales y de manera coherente con otras formas de comunicación comercial profesional. Todos los archivos adjuntos salientes se analizan automáticamente en busca de virus y códigos maliciosos. La transmisión de un archivo adjunto dañino no solo puede dañar el sistema del destinatario, sino también dañar la reputación de Bionica Automations. Las siguientes actividades están prohibidas por la política:

Envío de correo electrónico que pueda considerarse intimidatorio, acosador u ofensivo. Esto incluye, pero no se limita a: lenguaje abusivo, comentarios o imágenes sexualmente explícitos, blasfemias, comentarios difamatorios o discriminatorios con respecto a la raza, credo, color, sexo, edad, religión, orientación sexual, origen nacional o discapacidad.

* Usar el correo electrónico para realizar negocios personales.
* Usar el correo electrónico con el fin de enviar SPAM u otras solicitudes no autorizadas.
* Violar las leyes de derechos de autor mediante la distribución ilegal de obras protegidas.
* Enviar correo electrónico utilizando la cuenta de correo electrónico de otra persona, excepto cuando esté autorizado a enviar mensajes para otra persona mientras se desempeña en una función de apoyo administrativo.
* Crear una identidad falsa para eludir la política.
* Falsificar o intentar falsificar mensajes de correo electrónico.
* Usar software de correo electrónico no autorizado.
* Deshabilitar a sabiendas el escaneo automático de archivos adjuntos en cualquier computadora personal de Bionica Automations.
* Eludir a sabiendas las medidas de seguridad del correo electrónico.
* Enviar o reenviar correos electrónicos de broma, cartas en cadena o cartas falsas.
* Envío de mensajes no solicitados a grupos grandes, excepto cuando sea necesario para realizar negocios de Bionica Automations.
* Envío de mensajes o archivos adjuntos excesivamente grandes.
* Enviar o reenviar a sabiendas correos electrónicos con virus informáticos.
* Configurar o responder en nombre de Bionica Automations sin la aprobación de la gerencia.

Todo el material confidencial o sensible de Bionica Automations transmitido por correo electrónico, fuera de la red de Bionica Automations, debe estar encriptado. Las contraseñas para descifrar los datos no deben enviarse por correo electrónico.

El correo electrónico no es seguro. Los usuarios no deben enviar por correo electrónico contraseñas, números de la seguridad social, números de cuenta, números PIN, fechas de nacimiento, apellido de soltera de la madre, etc. a terceros fuera de la red de Bionica Automations sin cifrar los datos. Toda la actividad de los usuarios en los activos del sistema de información de Bionica Automations está sujeta a registro y revisión. Bionica Automations cuenta con software y sistemas para controlar el uso del correo electrónico.

Los usuarios de correo electrónico no deben dar la impresión de que representan, dan opiniones o hacen declaraciones en nombre de Bionica Automations, a menos que estén debidamente autorizados (explícita o implícitamente) para hacerlo.

Los usuarios no deben enviar, reenviar ni recibir información confidencial o sensible de Bionica Automations a través de cuentas de correo electrónico que no sean de Bionica Automations. Los ejemplos de cuentas de correo electrónico que no son de Bionica Automations incluyen, entre otros, Hotmail, correo de Yahoo, correo de AOL y correo electrónico proporcionado por otros proveedores de servicios de Internet (ISP). Los usuarios con dispositivos móviles que no sean de Bionica Automations deben cumplir con la Política de seguridad y uso aceptable de dispositivos personales para enviar, reenviar, recibir o almacenar información confidencial o sensible de Bionica Automations.

## Uso incidental

El uso personal incidental del envío de correo electrónico está restringido a los usuarios aprobados por Bionica Automations; no se extiende a familiares u otros conocidos. Sin la aprobación previa de la gerencia, el uso incidental no debe generar costos directos para Bionica Automations. El uso incidental no debe interferir con el desempeño normal de las funciones laborales de un empleado.

No se pueden enviar ni recibir archivos o documentos que puedan causar responsabilidad legal o vergüenza para Bionica Automations. El almacenamiento de archivos y documentos personales dentro de los sistemas de TI de Bionica Automations debe ser nominal.

## Retención de correos

Los mensajes se conservan durante 36 meses. Los correos electrónicos con más de 36 meses de antigüedad están sujetos a una depuración automática.

Los correos electrónicos eliminados y archivados están sujetos a una depuración automática.

## Archivado de correos

Solo el propietario de un buzón y el administrador del sistema tienen acceso al archivo.

Los mensajes se eliminarán del archivo en línea 36 meses después de la fecha original de envío/recepción.

# Actualizaciones

## Resumen

Las actualizaciones del software son uno de los puntos clave en cuanto a la seguridad informática. Desde Bionica Automations nos comprometemos a mantener actualizados nuestros equipos de trabajo para mejorar la seguridad de la red corporativa.

## Propósito

Concienciar a los trabajadores Bionica Automations sobre la importancia de mantener los sistemas actualizados.

## Audiencia

Esta política es aplicable a todo el personal de Bionica Automations que posea un equipo de trabajo o cualquier otro dispositivo electrónico con acceso a la red corporativa.

## Detalles de la política

Bionica Automations recomienda aplicar los últimos parches que salgan por lo menos una vez al mes.

Bionica Automations recomienda siempre tener actualizadas las aplicaciones de trabajo como pueden ser:

* El navegador web
* El cliente de correo electrónico
* El sistema operativo

# Redes sociales

## Descripción

El uso de redes sociales externas (es decir, Facebook, LinkedIn, Twitter, YouTube, etc.) dentro de las organizaciones con fines comerciales está aumentando. Bionica Automations se enfrenta a la exposición de cierta cantidad de información que puede ser visible para los amigos de los amigos de las redes sociales. Si bien esta exposición es un mecanismo clave que impulsa el valor, también puede crear un conducto inapropiado para que la información pase entre contactos personales y comerciales. Las herramientas para establecer barreras entre las redes personales y privadas y las herramientas para administrar cuentas de forma centralizada apenas están comenzando a surgir. La participación del Departamento de TI en cuestiones de seguridad, privacidad y ancho de banda es de suma importancia.

**Propósito de las redes sociales**

* **Crear una imagen positiva:** Bionica Automations puede usar las redes sociales para promover una imagen positiva. Si bien esto es particularmente importante para las organizaciones generalmente vulnerables a la prensa negativa o al descontento de los consumidores, también se puede usar para mejorar la imagen de Bionica Automations dentro de la comunidad.
* **Aumento de la participación mental:** las redes sociales pueden llegar a grandes audiencias a un costo monetario muy bajo, brindando a Bionica Automations otro medio para la promoción y el aumento de la conciencia de Bionica Automations.
* **Mejorar la satisfacción de los socios:** Los socios que reciben un servicio más oportuno y personal, en el medio que ellos prefieren, estarán más satisfechos.
* **Obtener información de los miembros:** las redes sociales se pueden usar para monitorear la opinión pública sobre Bionica Automations, sus productos y servicios, o sus competidores.
* **Aumentar la retención de miembros:** el uso de las redes sociales genera afinidad y lealtad, ya que los miembros se comprometen con un medio que prefieren: algo que Bionica Automations necesita ofrecer para seguir siendo competitivo.
* **Aumento de los ingresos:** uso de las redes sociales para crear aplicaciones de red personalizadas (también conocidas como complementos) para la promoción de productos o la integración con los servicios en línea de Bionica Automations.
* **Adquisición de miembros:** Uso de las redes sociales para responder rápida y eficientemente a los problemas de servicio a los miembros. La respuesta al problema puede ser pública, lo que permite que otros miembros que tengan la misma solicitud puedan buscarla.
* **Recuperación ante desastres:** uso de las redes sociales para eliminar temores de manera rápida y eficiente y comunicar información precisa sobre las acciones de recuperación en caso de un desastre.

## Detalles de la política

Bionica Automations fomenta el uso de las redes sociales como un canal para la comunicación comercial, de acuerdo con la estrategia de comunicación y marketing corporativo de BCHHU. Es política de Bionica Automations establecer pautas para el uso seguro de las redes sociales con respecto a la protección de la información de Bionica Automations. La seguridad y confidencialidad de la información es vital para el éxito de Bionica Automations. Bionica Automations ha establecido esta política para establecer parámetros y controles relacionados con el uso de sitios web de redes sociales por parte de Bionica Automations.

**Términos y condiciones de uso**

Todas las solicitudes para el uso de redes sociales externas por parte de un empleado de Bionica Automations, en nombre de Bionica Automations, deben enviarse al Equipo Directivo Superior. Bionica Automations puede permitir el acceso a determinados sitios web de redes sociales preaprobados. Los funcionarios de Bionica Automations solo pueden acceder a estos sitios de una manera consistente con los protocolos de seguridad de Bionica Automations y los funcionarios de Bionica Automations no pueden eludir los protocolos de seguridad de TI para acceder a los sitios de redes sociales.

**Está prohibido el uso de cuentas personales de redes sociales e identificaciones de usuario para Bionica Automations.**

Se prohíbe el uso de ID de usuario de redes sociales de Bionica Automations para uso personal. Está prohibido el uso de las direcciones de correo electrónico de Bionica Automations para registrarse en redes sociales, blogs u otras herramientas en línea utilizadas para uso personal. Los ejemplos de uso prohibido de las identificaciones de usuario de la empresa incluyen:

* Descargar e instalar complementos o aplicaciones auxiliares, como las que intentan acceder al directorio de correo electrónico de Bionica Automations
* Unirse a grupos utilizando una identificación de usuario de la empresa por motivos personales
* Agregar amigos personales a la lista de amigos de un oficial de Bionica Automations
* Los funcionarios de Bionica Automations deben reconocer que han revisado los Términos de servicio o los Términos de usuario del servicio de redes sociales, según corresponda. Los enlaces para los sitios están abajo.

**Representando a Bionica Automations**

La alta gerencia de Bionica Automations designará a una persona o equipo para administrar y responder a los problemas de las redes sociales relacionados con Bionica Automations y determinará quién tendrá la autoridad para contribuir con el contenido. Las responsabilidades de esta(s) persona(s) incluirán, pero no se limitarán a:

* **Gestión** de herramientas y canales de redes sociales;
* **Responder** a preguntas internas y externas sobre el sitio de redes sociales;
* **Abordar** problemas/brindar orientación al personal si un usuario se vuelve amenazante, abusivo o acosador;
* **Sugerir** cambios a esta política de medios sociales de Bionica Automations cuando se justifique;
* **Trabajar** con otros miembros del personal para asegurarse de que no se pasen por alto las oportunidades en la comercialización de los servicios de Bionica Automations; y
* **Capacitar** al personal para garantizar que entiendan cómo usar el programa de redes sociales de Bionica Automations.

Bionica Automations tomará las medidas necesarias para asegurarse de que el contenido cumpla con las leyes y regulaciones aplicables.

Se espera que todos los empleados de Bionica Automations que participan en las redes sociales, en nombre de Bionica Automations, representen a Bionica Automations de manera profesional. De lo contrario, podría tener un impacto negativo en Bionica Automations y podría poner en peligro la capacidad de un empleado de Bionica Automations para participar en las redes sociales en el futuro.

Bionica Automations es propietaria de todo el contenido de redes sociales y redes sociales autorizado. Los funcionarios de Bionica Automations tienen prohibido tomar, guardar o enviar cualquier contenido de Bionica Automations distribuido a través de las redes sociales mientras estén empleados, separados, sirviendo en la Junta Directiva o despedidos por Bionica Automations.

Las nuevas tecnologías y herramientas de redes sociales evolucionan continuamente. A medida que surjan nuevas herramientas, esta política se actualizará para reflejar los cambios.

Las plataformas para la colaboración en línea están cambiando fundamentalmente el entorno de trabajo y ofrecen nuevas formas de interactuar con los miembros y la comunidad. Se deben seguir los principios rectores para participar en las redes sociales.

* Publique comentarios significativos y respetuosos y absténgase de hacer comentarios fuera de tema u ofensivos.
* Responda a los comentarios rápidamente cuando la respuesta sea adecuada.
* Conozca y siga las leyes estatales y federales que protegen la confidencialidad de los miembros en todo momento.
* Proteger la información de propiedad exclusiva y la confidencialidad.
* Cuando no esté de acuerdo con las opiniones de los demás, manténgalo profesional.
* Conocer el Código de Conducta de Bionica Automations y aplicar los estándares y principios en computación social.

**Blogs personales y posts**

Bionica Automations no se pronuncia sobre la decisión de un empleado de Bionica Automations de iniciar o mantener un blog o sitio web personal o de participar en otras actividades de redes sociales en línea fuera del trabajo. Los funcionarios de Bionica Automations, que se identifican como funcionarios de Bionica Automations en una red social, deben asegurarse de que su perfil y el contenido relacionado sean coherentes con la forma en que ellos y Bionica Automations desean que se presenten. Esto incluye lo que el empleado de Bionica Automations escribe sobre sí mismo y el tipo de fotos que publica.

Los funcionarios de Bionica Automations no deben revelar información patentada y deben tener cuidado con la publicación de exageraciones, obscenidades u otras caracterizaciones que puedan provocar litigios.

Los funcionarios de Bionica Automations no deben hacer referencia pública a ningún procedimiento de seguridad o efectivo relacionado con Bionica Automations.

Los funcionarios de Bionica Automations que comenten sobre cualquier problema comercial o de política de Bionica Automations deben identificarse claramente como funcionarios de Bionica Automations en su blog o publicación e incluir un descargo de responsabilidad de que las opiniones son propias y no de Bionica Automations. Al generar contenido relacionado con Bionica Automations o personas asociadas con Bionica Automations, los funcionarios de Bionica Automations deben usar un descargo de responsabilidad como "Las publicaciones en este sitio son mías y no necesariamente reflejan las opiniones de Bionica Automations".

Los funcionarios de Bionica Automations no deben utilizar los sitios web de redes sociales para acosar, amenazar, discriminar, menospreciar o difamar a cualquier otro funcionario, miembro, proveedor, producto, servicio o filosofía comercial de Bionica Automations.

Los empleados de Bionica Automations tienen prohibido divulgar información comercial o personal confidencial, patentada o confidencial relacionada con Bionica Automations o cualquiera de sus empleados, proveedores o miembros de Bionica Automations. Los funcionarios de Bionica Automations también tienen prohibido divulgar cualquier información comercial o personal confidencial, patentada o sensible que pueda identificar a otro funcionario, proveedor o miembro de Bionica Automations sin la autorización previa de esa persona.

Los empleados de Bionica Automations no deben realizar ninguna acción a través de sitios web de redes sociales o blogs personales que puedan dañar, o puedan dañar, la reputación de Bionica Automations o cualquier empleados, miembro o proveedor de Bionica Automations.

**Reglas de escritura**

* Los funcionarios de Bionica Automations deben escribir y publicar sobre sus áreas de especialización, especialmente en lo que se refiere a Bionica Automations.
* Escribe en primera persona. Hable con el lector como si fuera una persona real en una situación profesional.
* Evite un lenguaje demasiado compuesto.
* Considere el contenido que es abierto e invita a la respuesta.
* Fomente los comentarios.
* Utilice un corrector ortográfico.
* Haga el esfuerzo de ser claro, completo y conciso en la comunicación. Determine si el material se puede acortar o mejorar.
* Si se comete un error, debe reconocerse. Sea sincero y sea rápido con la corrección. Si publica en un blog, aclare si se ha realizado una modificación en una publicación anterior.

Produce material que los miembros de Bionica Automations valorarán. La comunicación en las redes sociales de Bionica Automations debería ayudar a sus miembros, socios y compañeros de trabajo. se debe pensar

provocando y construyendo un sentido de comunidad. Debería ayudar a los miembros a mejorar su conocimiento o comprender mejor a Bionica Automations o a un afiliado.

El contenido anónimo no está permitido en los sitios de Bionica Automations.

**Uso personal de sitios de terceros durante el horario laboral**

El correo electrónico y el acceso a Internet se proporcionan para respaldar los fines comerciales de Bionica Automations. Si se accede a estas herramientas, se permite el uso personal incidental de las mismas. En general, Bionica Automations limitará el acceso a los sitios de redes sociales a los funcionarios de Bionica Automations que lo usan en nombre de Bionica Automations. No se permite el uso personal excesivo de cualquier herramienta de Internet durante el tiempo de trabajo y los privilegios de acceso pueden ser revocados por abuso del sistema.

**Las represalias están prohibidas**

Bionica Automations prohíbe tomar medidas negativas contra cualquier funcionario de Bionica Automations por informar una posible desviación de esta política o por cooperar en una investigación. Cualquier funcionario de Bionica Automations que tome represalias contra otro funcionario de Bionica Automations por informar una posible desviación de esta política o por cooperar en una investigación estará sujeto a medidas disciplinarias, que pueden incluir el despido en Bionica Automations o remoción de la Junta Directiva.