MAESTRÍA EN CIBERSEGURIDAD

PROYECTO DE TITULACIÓN

Modalidad Proyecto de Investigación y Desarrollo

Creación e Implementación de Normas y Políticas Para el Uso Correcto del Correo Empresarial

Autor: Hamilton Roger Gómez Villafuerte

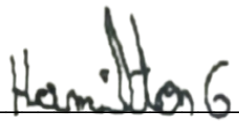
Guía: Roque Jacinto Hernández Bustos

Presentando como parte de los requisitos para el título de magister en ciberseguridad.

Guayaquil,29 de Febrero del 2024

PROPUESTA DE CLÁUSULA DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TRABAJOS DE TITULACIÓN

Yo, GÓMEZ VILLAFUERTE, HAMILTON ROGER, autor del trabajo de titulación "Creación e Implementación De Normas y Políticas Para el Uso Correcto del Correo Empresarial", certifico que el ensayo reflexivo es una creación de mi autoría, por lo que sus contenidos son originales, de exclusiva responsabilidad de su autor y no infringen derechos de autor de terceras personas. Con lo cual, exonero a la Universidad Casa Grande de reclamos o acciones legales.

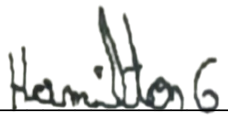


GÓMEZ VILLAFUERTE, HAMILTON ROGER

0929470938

GÓMEZ VILLAFUERTE, HAMILTON ROGER en calidad de autor y titular del trabajo de titulación "Creación e Implementación De Normas y Políticas Para el Uso Correcto del Correo Empresarial" para optar por la **Maestría en Ciberseguridad**, autorizo a la Universidad Casa Grande para que realice la digitalización y publicación de este trabajo de titulación en su Repositorio Digital de acceso abierto, con fines estrictamente académicos, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Asimismo, autorizo a la Universidad Casa Grande a reproducir, distribuir, comunicar y poner a disposición del público mi documento de trabajo de titulación en formato físico o digital y en cualquier medio sin modificar su contenido, sin perjuicio del reconocimiento que deba hacer la Universidad sobre la autoría de dichos trabajos.



GÓMEZ VILLAFUERTE, HAMILTON ROGER

0929470938

Introducción

En la era digital actual, donde la tecnología desempeña un papel central en prácticamente todos los aspectos de nuestras vidas, la ciberseguridad se ha convertido en un tema crítico y de creciente relevancia. La ciberseguridad se refiere a las medidas, prácticas y tecnologías diseñadas para proteger sistemas, redes y datos contra ataques cibernéticos, intrusiones maliciosas y vulnerabilidades potenciales. Desde el robo de identidad hasta el ransomware y los ataques de denegación de servicio (DDoS), las amenazas cibernéticas son cada vez más sofisticadas y pueden tener consecuencias devastadoras para individuos, empresas e incluso infraestructuras gubernamentales.

"Además, según el estudio realizado por cisco en el año 2019; en su reporte de amenazas señala que a partir del año 2016 el uso de ransomware era unos de los principales métodos de ciberataque; y que a principios del 2018 este método está quedando para la historia, pero esto no quiere decir que se tiene que pasar por alto." (García, 2021)

En la actualidad, la ciberseguridad se ha convertido en un tema de vital importancia para empresas y organizaciones de todas las industrias. Con el crecimiento exponencial de las amenazas cibernéticas, es fundamental contar con medidas de seguridad efectivas para proteger la información sensible y los activos de una empresa. La ciberseguridad abarca un amplio espectro de técnicas y herramientas diseñadas para prevenir, detectar y responder a posibles ataques informáticos, protegiendo así la integridad, confidencialidad y disponibilidad de los datos.

"Según un informe del portal web de grupo semana sobre las tendencias de seguridad, para los colombianos las principales preocupaciones también incluyen

amenazas de ingeniería social, llamadas phishing, con un 56%, a través del cual el adulto mayor es engañado al hacerle creer que ingresa a un sitio seguro cuando no lo es. Con este mismo porcentaje (56%), las empresas temen los ataques de negación del servicio (dos), que atacan directamente un sistema informático o una red, lo que lo hace inaccesible para sus empleados. Y los peligros asociados con el Ransomware, mejor conocido como "secuestro de datos" con un (34%).6". (Camilo, 2023)

En resumen, la ciberseguridad es esencial en un mundo interconectado y digitalizado, donde los datos y la información son activos críticos que deben protegerse contra una variedad de amenazas cibernéticas en constante evolución. Desde individuos hasta grandes corporaciones, la seguridad en línea es una responsabilidad compartida que requiere una combinación de tecnología avanzada, buenas prácticas de seguridad y una mentalidad proactiva para hacer frente a los desafíos emergentes en el panorama cibernético actual.

Breve descripción del proyecto

En el entorno empresarial moderno, el correo electrónico es una herramienta vital para la comunicación y el intercambio de información. Sin embargo, la seguridad del correo electrónico es una preocupación fundamental debido a la creciente sofisticación de las amenazas cibernéticas. Este proyecto de políticas de seguridad tiene como objetivo establecer un marco sólido para proteger la integridad, confidencialidad y disponibilidad de los correos electrónicos empresariales.

Otro aspecto importante es la encriptación de correos electrónicos. La encriptación garantiza que el contenido del correo no pueda ser leído por personas no autorizadas durante su transmisión. Esto es especialmente importante cuando se trata de

información sensible o confidencial, ya que evita que los terceros intercepten y accedan a los datos.

Por último, es fundamental educar y concientizar a los empleados sobre las mejores prácticas de seguridad en el correo empresarial. Esto implica capacitación regular sobre cómo reconocer y evitar correos electrónicos de phishing, cómo manejar archivos adjuntos sospechosos y cómo reportar cualquier actividad sospechosa. Adicionalmente, se deben tratar las políticas sobre el uso adecuado del correo electrónico y las consecuencias de violar estas políticas.

En resumen, las políticas de seguridad en el correo empresarial son fundamentales para proteger la información y garantizar la confidencialidad en el entorno laboral. Establecer contraseñas sólidas, implementar encriptación y educar a los empleados sobre algunas de las medidas claves para un correo electrónico seguro y confiable.

“La seguridad en informática es un aspecto fundamental en nuestro entorno de trabajo, hogares, escuelas, etc. una actividad al que no se le debe de escatimar en dinero y tiempo que más adelante nos ayudara a mitigar el impacto y los riesgos a los que puedan estar expuestos nuestros equipos y redes.” (Rivera, 2023)

Materias que fueron fundamentales para el proyecto

Para este proyecto se escogieron estas materias las cuales fueron fundamentales para poder llevarlo a cabo.

Continuidad de Negocio

La Continuidad de Negocio es una disciplina fundamental para garantizar que una organización pueda mantener sus operaciones vitales en funcionamiento incluso después de enfrentar interrupciones o desastres. Al considerar la seguridad del correo empresarial, la perspectiva de la Continuidad de Negocio puede ofrecer una serie de beneficios y enfoques útiles para elaborar protocolos sólidos

- Evaluación de riesgos y análisis de impacto
- Desarrollo de planes de respuesta ante incidentes
- Pruebas y ejercicios de simulación

Además, la continuidad del negocio también incluye la realización de pruebas y simulacros para evaluar la efectividad de los protocolos de seguridad establecidos. Estas pruebas pueden ayudar a identificar vulnerabilidades en el correo empresarial y a corregirlas antes de que se conviertan en un problema grave para la empresa. En definitiva, la materia de continuidad de negocio puede ser de gran ayuda para elaborar protocolos de seguridad en el correo empresarial que sean eficaces, robustos y adaptables a las necesidades y riesgos específicos de la organización.

En resumen, al integrar los principios y prácticas de la Continuidad de Negocio en el desarrollo de protocolos de seguridad para el correo empresarial, las organizaciones pueden mejorar su capacidad para protegerse contra amenazas cibernéticas y mantener la continuidad de sus operaciones comerciales incluso en situaciones adversas.

Seguridad de Aplicaciones y Bases de Datos

La seguridad de aplicaciones y bases de datos es un aspecto clave en la protección de la información sensible de una empresa, ya que tanto las aplicaciones como las bases de datos almacenan y procesan datos críticos para el funcionamiento de la organización. Al implementar políticas de seguridad en el correo electrónico, la seguridad de aplicaciones y bases de datos puede ser de gran ayuda, ya que estas políticas pueden complementarse con medidas adicionales para garantizar la integridad, confidencialidad y disponibilidad de la información que se intercambia a través de este medio.

En otro orden de ideas, podemos decir que la seguridad de aplicaciones y bases de datos puede proporcionar una base sólida para implementar políticas de seguridad en el correo electrónico, ya que comparten muchos principios y enfoques comunes en la protección de datos y la mitigación de riesgos. Aquí hay algunas formas en que la seguridad de aplicaciones y bases de datos puede ayudar en la implementación de políticas de seguridad de correo

- Cifrado y firma digital
- Desactivar el formato HTML
- Aplicaciones antimalware y filtros antispam
- Protección de contraseñas

En resumen, la seguridad de aplicaciones y bases de datos puede ser un componente esencial para fortalecer las políticas de seguridad en el correo electrónico, proporcionando una capa adicional de protección a la información crítica de la empresa. Al integrar estas áreas de seguridad, se puede crear un entorno más seguro y robusto para la gestión del correo empresarial y para la protección de la información confidencial de la organización.

Estrategia y Políticas Multilaterales para la Ciberseguridad

Las estrategias y políticas multilaterales para la ciberseguridad pueden ser de gran ayuda en la implementación de políticas de seguridad del correo electrónico, ya que proporcionan un marco de referencia y lineamientos internacionales que pueden ser adaptados por las organizaciones para fortalecer su seguridad cibernética. Al seguir estas estrategias y políticas, las empresas pueden mejorar su protección contra amenazas cibernéticas y garantizar la confidencialidad, integridad y disponibilidad de la información que se envía y recibe a través del correo electrónico.

Uno de los beneficios de las estrategias y políticas multilaterales para la ciberseguridad es que suelen incluir mejores prácticas y recomendaciones basadas en la experiencia y conocimientos de expertos en seguridad cibernética a nivel mundial. Esto puede ayudar a las empresas a identificar posibles vulnerabilidades en sus sistemas de correo electrónico y a implementar medidas de protección más efectivas y actualizadas. Además, alinearse con estas políticas internacionales puede mejorar la credibilidad de la organización en cuanto a su compromiso con la seguridad cibernética.

En resumen, al seguir las estrategias y políticas multilaterales para la ciberseguridad, las organizaciones pueden mejorar su capacidad para proteger el correo electrónico y la información crítica que se intercambia a través de este medio. Al implementar políticas de seguridad del correo electrónico en línea con las recomendaciones internacionales, las empresas pueden fortalecer su postura de seguridad cibernética y mitigar los riesgos asociados con posibles ataques informáticos.

Gerencia, Operación y planificación de la ciberseguridad

La gerencia, operación y planificación de la ciberseguridad juegan un papel crucial en la implementación de normas y políticas para el uso correcto del correo empresarial. Aquí hay algunas formas en que estas áreas pueden contribuir a este proceso:

Gerencia: Establecimiento de objetivos y prioridades: La gerencia en ciberseguridad puede definir los objetivos estratégicos y las prioridades relacionadas con el uso seguro del correo empresarial.

Asignación de recursos: La gerencia puede asignar los recursos necesarios, ya sean financieros, humanos o tecnológicos, para implementar y hacer cumplir las normas y políticas de seguridad del correo empresarial

Supervisión y cumplimiento: La gerencia es responsable de supervisar el cumplimiento de las normas y políticas establecidas, así como de tomar medidas correctivas cuando sea necesario.

Implementación técnica: El equipo de operaciones de ciberseguridad es responsable de implementar las medidas técnicas necesarias para hacer cumplir las normas y políticas de seguridad del correo empresarial.

Monitoreo y respuesta a incidentes: Las operaciones de ciberseguridad también involucran monitorear continuamente el tráfico de correo electrónico en busca de actividades sospechosas y responder rápidamente a incidentes de seguridad

Planificación: Evaluación de riesgos: La planificación de la ciberseguridad implica la evaluación regular de los riesgos asociados con el correo empresarial, identificando vulnerabilidades y amenazas potenciales.

En resumen, la gerencia, operación y planificación de la ciberseguridad son fundamentales para implementar normas y políticas para el uso correcto del correo empresarial. Esto implica desarrollar políticas de seguridad, implementar medidas técnicas de protección y planificar la respuesta a incidentes. Al seguir estas prácticas, las organizaciones pueden fortalecer la seguridad de su correo electrónico y proteger la información confidencial de posibles amenazas cibernéticas.

Ciberseguridad Ubicua

La ciberseguridad ubicua juega un papel fundamental en la implementación de normas y políticas para el uso correcto del correo empresarial, ya que garantiza la protección de la información en cualquier momento y lugar, independientemente de la ubicación de los usuarios o de los dispositivos desde los que acceden al correo electrónico de la empresa. Al contar con ciberseguridad ubicua, se puede asegurar que se sigan las políticas de seguridad del correo empresarial, evitando así posibles brechas de seguridad. Aquí hay algunas formas en las que puede ayudar:

- Concientización y capacitación en ciberseguridad
- Implementación de medidas de seguridad técnicas
- Desarrollo de políticas de seguridad

En resumen, la ciberseguridad ubicua puede ayudar en la implementación de normas y políticas para el uso correcto del correo empresarial al promover la concientización y capacitación en ciberseguridad, implementar medidas técnicas de seguridad y desarrollar políticas de seguridad claras. Estas medidas contribuyen a proteger la información confidencial y garantizar un uso seguro del correo empresarial.

Implementación

Se estima implementar un software lo cual pueda filtrar los correos y evitar fuga de información. Adicionalmente, se van a crear normas y políticas que los empleados deben cumplir. De esta manera, el software acompañado de las normas, crean una seguridad de ambas partes y de esa forma llevar un correcto uso de la información obtenida por parte del paciente y así evitar algún inconveniente a largo plazo de fuga de información.

Por medio del correo electrónico se maneja mucha información primordial para el giro de negocio, que actualmente se encuentra propuesto este proyecto, que es de una clínica oftalmológica. Las investigaciones recientes respecto al tema citado muestran que por medio del servicio de correo se recepta y se envía mucha información y documentación muy delicada y confidencial. Si este sistema llega a ser vulnerado podría llevar a una filtración de información del paciente como, por ejemplo:

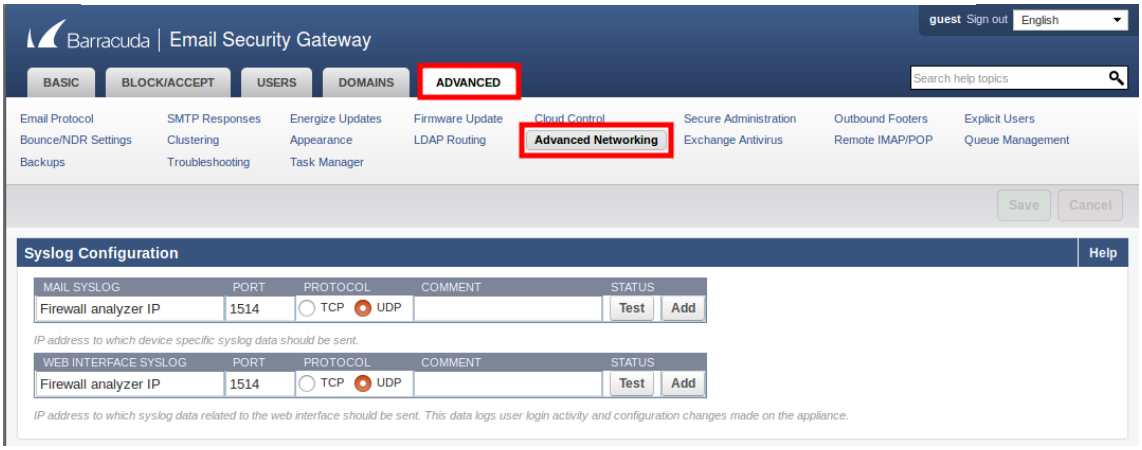
- Exámenes de laboratorio
- Cédula de ciudadanía
- Firmas electrónicas
- Coberturas del seguro para atención

Asimismo, mucha información adicional que es muy primordial para la clínica y el paciente.

Los controles que se va a implementar son basados en un estudio de campo y el comportamiento de usuario que pudo evidenciar muchas falencias por lo cual se recomienda la implementación de un software llamado:

Barracuda Email Security Gateway

Es una solución de seguridad de correo electrónico basada en la nube o en un dispositivo físico que ayuda a proteger las organizaciones contra amenazas en los correos electrónicos, como malware, phishing, spam y ataques de ingeniería social. Esta solución ofrece diversas características y funcionalidades que ayudan a proteger la información confidencial de la empresa y a garantizar la integridad de las comunicaciones por correo electrónico.



En resumen, el Barracuda Email Security Gateway es una solución integral de seguridad de correo electrónico que ayuda a proteger a las organizaciones contra amenazas en los correos electrónicos. Su uso adecuado y configuración personalizada pueden contribuir significativamente a reforzar la ciberseguridad de una organización.

Conclusión

El principal objetivo de la implementación de normas y políticas para el uso correcto del correo empresarial en una clínica es esencial para proteger la información confidencial, prevenir amenazas cibernéticas, cumplir con las regulaciones y mejorar la productividad. Estas normas deben incluir pautas sobre el manejo seguro de la información, la identificación de correos electrónicos sospechosos y el uso adecuado de los recursos de la clínica.

En resumen, aplicar normas y políticas para el uso correcto del correo empresarial es esencial para proteger los activos digitales, prevenir amenazas cibernéticas, cumplir con regulaciones legales y fomentar una cultura organizacional segura y consciente en materia de ciberseguridad.

Limitaciones

Existen varias limitaciones que pueden surgir durante la implementación de normas y políticas para el uso correcto del correo empresarial. Algunas de las limitaciones comunes pueden incluir:

Falta de recursos

La implementación de medidas de seguridad adicionales, como soluciones de cifrado de correos electrónicos o autenticación de dos factores, puede requerir recursos adicionales, tanto en términos de tiempo como de inversión económica.

Tecnología obsoleta

Si la empresa utiliza sistemas de correo electrónico obsoletos o no actualizados, puede ser más difícil implementar ciertas medidas de seguridad avanzadas, lo que limitaría la efectividad de las normas y políticas establecidas.

A pesar de estas limitaciones, es crucial superar estos desafíos para garantizar la protección de la información confidencial, prevenir amenazas cibernéticas y cumplir con las regulaciones legales en el uso del correo empresarial. Al abordar estas limitaciones con una planificación adecuada, comunicación efectiva y capacitación continua, las empresas pueden implementar con éxito normas y políticas que fortalezcan la seguridad en el uso del correo electrónico.

Recomendación Adicional

Se ha determinado que pueden ocurrir pérdidas de información si no se toman los correctivos del sistema donde se almacenan al paciente e ingresan los valores recaudados.

Con respecto a la información almacenada, conversando con el área contable al término de la jornada, se estima que la clínica percibe diariamente un monto de 20.000 dólares. Se estima que si hubiera un problema de denegación de servicio (DOS), lo que podría limitar el uso de la plataforma donde se ingresa los paciente y valores a cobrar tendríamos una pérdida con solo 8 días de 160.000 dólares.

Estos son valores relativamente altos que adicionalmente llevarían a perder credibilidad e imagen por ende se recomienda una revisión al sistema que actualmente se maneja donde se a evidencia algunas brechas de vulnerabilidad.

DÍAS		VALORES DE PÉRDIDAS
1		20000
3		60000
5		100000
8		160000

Se recomienda una auditoría de la seguridad de la información del sistema para así poder ver que tan segura es la plataforma y poder prevenir cualquiera amenaza que podríamos experimentar.

Referencias

Camilo, M. R. C. (2023). Medidas preventivas de ciberseguridad que debe tener el adulto mayor en Colombia para acceder a internet y sus servicios. https://repository.unad.edu.co/handle/10596/59691

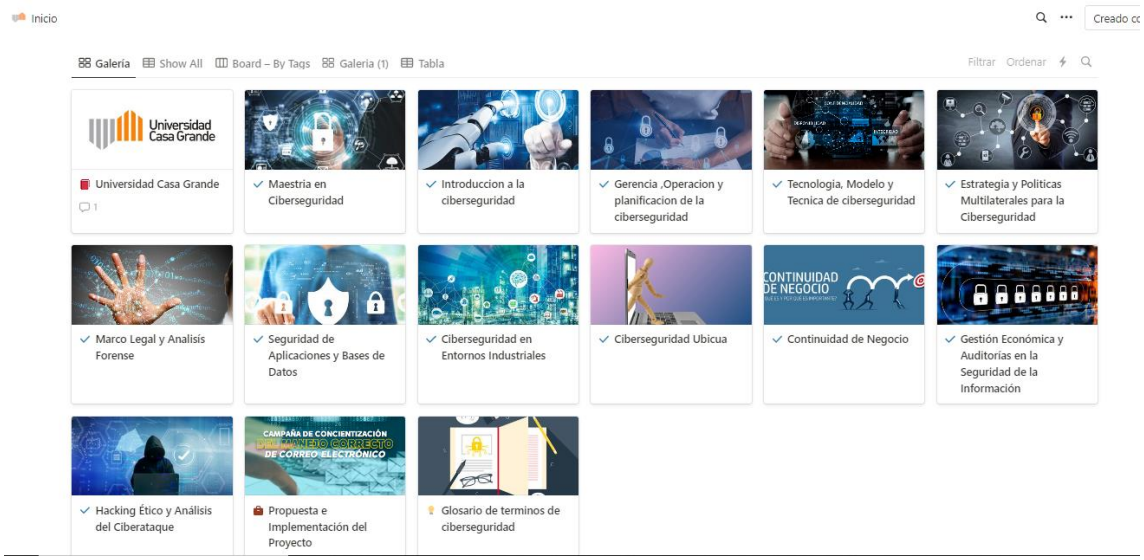
García Perero, F. G. (2021). *Análisis e implantación de técnicas y herramientas de ethical hacking para la Ciberseguridad* (Bachelor's thesis, La Libertad: Universidad Estatal Península de Santa Elena, 2021). https://repositorio.upse.edu.ec/handle/46000/5917

Rivera Nuñez, L. A. (2023). Inteligencia de amenazas basada en honeypots para una ciberseguridad oportuna en la nube. https://ri.uaemex.mx/handle/20.500.11799/140060

ANEXO 1

Enlace de Evidencias de Aprendizaje

https://tidy-roadway-c8a.notion.site/7b49037dd0484bc8828a6e2d24bf768d?v=bb0439dee91e459787c2ec51b5bd5742&pvs=4

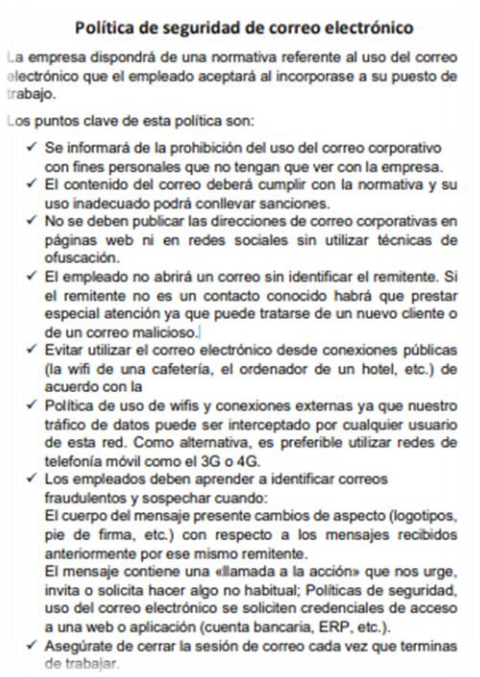


ANEXO 2

Propuesta de implementación

https://tidy-roadway-c8a.notion.site/Propuesta-e-Implementaci-n-del-Proyecto-5cd8206f83514da4b2533acd4d77b304

En esta guía, exploraremos los aspectos clave de las políticas de seguridad de correo electrónico, desde la autenticación y cifrado hasta la concientización del usuario y la gestión de riesgos. Entender y aplicar estas políticas no solo fortalecerá la seguridad de las comunicaciones por correo electrónico, sino que también contribuirá a la protección de la información sensible y la reputación de las organizaciones en un panorama digital cada vez más complejo y amenazante.



Política de seguridad de correo electrónico

La empresa dispondrá de una normativa referente al uso del correo electrónico que el empleado aceptará al incorporase a su puesto de trabajo.

Los puntos clave de esta política son:

- ✓ Se informará de la prohibición del uso del correo corporativo con fines personales que no tengan que ver con la empresa.
- ✓ El contenido del correo deberá cumplir con la normativa y su uso inadecuado podrá conllevar sanciones.
- ✓ No se deben publicar las direcciones de correo corporativas en páginas web ni en redes sociales sin utilizar técnicas de ofuscación.
- ✓ El empleado no abrirá un correo sin identificar el remitente. Si el remitente no es un contacto conocido habrá que prestar especial atención ya que puede tratarse de un nuevo cliente o de un correo malicioso.
- ✓ Evitar utilizar el correo electrónico desde conexiones públicas (la wifi de una cafetería, el ordenador de un hotel, etc.) de acuerdo con la
- ✓ Política de uso de wifis y conexiones externas ya que nuestro tráfico de datos puede ser interceptado por cualquier usuario de esta red. Como alternativa, es preferible utilizar redes de telefonía móvil como el 3G o 4G.
- ✓ Los empleados deben aprender a identificar correos fraudulentos y sospechar cuando:
  El cuerpo del mensaje presente cambios de aspecto (logotipos, pie de firma, etc.) con respecto a los mensajes recibidos anteriormente por ese mismo remitente.
  El mensaje contiene una «llamada a la acción» que nos urge, invita o solicita hacer algo no habitual; Políticas de seguridad, uso del correo electrónico se soliciten credenciales de acceso a una web o aplicación (cuenta bancaria, ERP, etc.).
- ✓ Asegúrate de cerrar la sesión de correo cada vez que terminas de trabajar.

Software a implementar de seguridad de correos

Barracuda Email Security Gateway

Una solución de seguridad de correo electrónico completa que bloquee los ataques originados por correos electrónicos y que, al mismo tiempo, proporcione las funciones adicionales necesarias para garantizar la continuidad del negocio por un precio asequible.

-Protección completa a largo plazo -Protección completa para amenazas de correo electrónico -Asequible y fácil de usar