UNIVERSIDAD DE LA SALLE

LINEAMIENTOS USO SEGURO DEL CORREO ELECTRÓNICO INSTITUCIONAL

DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN
Gestión de Tecnologías de la Información

Este documento corresponde a información exclusiva de la Universidad de la Salle asociada con los procesos y actividades dentro de la organización. Esta información no podrá ser reproducida total o parcialmente, salvo autorización expresa de la Universidad de La Salle.

TABLA DE CONTENIDO

1. OBJETIVO 3
2. ALCANCE 3
3. TÉRMINOS Y DEFINICIONES 3
4. DIRECTRICES GENERALES PARA EL USO SEGURO DE CORREO ELECTRÓNICO INSTITUCIONAL 4
4.1 Dirección de Tecnologías de Información y Comunicación 4
4.2 Dirección de Auditoría Interna 4
4.3 Usuario final 4
5. CONTROL DOCUMENTAL 6

1. OBJETIVO

Establecer los lineamientos que garanticen el control y uso seguro del correo electrónico institucional, el cual es administrado por Dirección de Tecnologías de Información y Comunicación, esto con el fin de evitar el mal uso de la herramienta y minimizar el riesgo de ataques que puedan afectar la integridad, disponibilidad y confidencialidad de la información.

2. ALCANCE

Aplica para todo el personal administrativo, docente, proveedores y terceros que tengan asignada una cuenta de correo institucional de Universidad de La Salle.

3. TÉRMINOS Y DEFINICIONES

Batch: Archivo de procesamiento por lotes, es un archivo de texto el cual no tiene un formato definido, estos archivos contienen instrucciones programadas para ser ejecutadas mediante un archivo con extensión .bat e interpretadas mediante sistema MS-DOS propio de Microsoft Windows.

Email Spoofing: El spoofing es una técnica utilizada por atacantes con intenciones maquiavélicas, que en una red de tecnología usurpan la identidad y se hace pasar por un ente distinto a través de falsificación de datos, esto se conoce comúnmente como “hacerse pasar por otro” el Web spoofing o el e-mail (smtp) spoofing, que es el conjunto de técnicas utilizadas para hacerse pasar por otro emisor en un correo electrónico (Molina Valdiviezo & Auquilla Guamantaqui, 2019).

Exe: Se refiere a un archivo el cual contiene instrucciones para iniciar una aplicación de software, para este ámbito puede incluir o no un código malicioso.

Spam: Es el uso abusivo de la tecnología de correo electrónico al inundar los buzones de usuarios con mensajes no solicitados (ENISA, threat landscape 2013, 2014).

Spammer: Tipo de usuario que suele generar gran cantidad de contenido no deseado por otros usuarios. Intención maliciosa o poco adecuada para tal entorno comúnmente de finalidad comercial. (Tauste Martí, 2018).

Phishing: Conjunto de técnicas que pretenden, sin conocimiento de la víctima, la consecución de datos especialmente sensibles (sobre todo bancarios) captándolos de un modo ilícito a través de falsos formularios o simulaciones de la página web de la empresa a la que se falsea. Las simulaciones de phishing se reciben principalmente vía mensajes de correo. (Hernando, 2005).

4. DIRECTRICES GENERALES PARA EL USO SEGURO DE CORREO ELECTRÓNICO INSTITUCIONAL

4.1 Dirección de Tecnologías de Información y Comunicación

- Estudiar y desplegar medidas de seguridad para la plataforma de correo, con el fin de proteger el posible ingreso de correos malintencionados que empleen las diferentes técnicas de ataque (spam, phishing, email- spoofing).
- Divulgar periódicamente con el apoyo de área de comunicaciones los lineamientos y recomendaciones de uso de adecuado de correo electrónico descritos en el presente documento.
- Impulsar con el apoyo de área de comunicaciones campañas de concientización dirigida a personal administrativo, docente y estudiantes, relacionadas con buenas prácticas y precauciones acerca del uso del correo electrónico.

4.2 Dirección de Auditoría Interna

Realizar auditorías periódicas a los controles implementados por Dirección de Tecnologías de Información y Comunicación.

4.3 Usuario final

- La cuenta de correo electrónico debe ser únicamente para uso institucional y actividades propias del desempeño del cargo y funciones asignadas dentro de la Universidad de la Salle, durante la relación contractual (funcionarios y docentes) y académica (estudiantes y egresados).
- En el caso que llegase a terminar la relación con la Universidad de conformidad con los procedimientos institucionales, la cuenta de correo electrónico @unisalle y @lasalle se eliminará y de ser del caso, si hay un reintegro se creará nuevamente con la misma dirección.
- El envío de información institucional debe ser realizado exclusivamente desde la cuenta de correo asignado por la Universidad de La Salle, por tal motivo, no se debe tratar información de ámbito institucional por medio de correos electrónicos personales (envío y recepción).
- La herramienta de correo electrónico debe ser usada de manera segura y ética, todos los usuarios son responsables de las actividades que se ejecuten con las credenciales de acceso de correo electrónico asignado, por lo cual, se deben adoptar practicas seguras las cuales eviten el compromiso de información almacenada en los buzones de correo.
- La cuenta de correo electrónico debe ser únicamente para uso institucional y actividades propias del desempeño del cargo y funciones asignadas dentro de la Universidad de la Salle, durante la relación contractual (funcionarios y docentes) y académica (estudiantes y egresados).
- En el caso que llegase a terminar la relación con la Universidad de conformidad con los procedimientos institucionales, la cuenta de correo electrónico @unisalle y @lasalle

se eliminará y de ser del caso, si hay un reintegro se creará nuevamente con la misma dirección.

- El envío de información institucional debe ser realizado exclusivamente desde la cuenta de correo asignado por la Universidad de La Salle, por tal motivo, no se debe tratar información de ámbito institucional por medio de correos electrónicos personales (envío y recepción).
- La herramienta de correo electrónico debe ser usada de manera segura y ética, todos los usuarios son responsables de las actividades que se ejecuten con las credenciales de acceso de correo electrónico asignado, por lo cual, se deben adoptar practicas seguras las cuales eviten el compromiso de información almacenada en los buzones de correo.

  "AVISO LEGAL:
  - Las opiniones expresadas en el presente mensaje no representan necesariamente la opinión oficial de La Universidad de La Salle.
  - Este mensaje es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas de su destinatario. Si obtiene esta transmisión por error, por favor destruya su contenido y avise al remitente. Está prohibida su retención, grabación, utilización o divulgación con cualquier propósito.
  - Este mensaje ha sido sometido a programas antivirus. No obstante, La Universidad de La Salle no asume ninguna responsabilidad por eventuales daños generados por el recibo y uso de este material, siendo responsabilidad del destinatario verificar con sus propios medios de la existencia de virus u otros defectos."

- No abrir ni responder correos electrónicos que contengan documentos o archivos adjuntos provenientes de direcciones desconocidas o que contengan un asunto u origen poco fiable, tampoco visitar los sitios web que recomienden allí.
- Se debe prestar atención a correos electrónicos con datos adjuntos sospechosos o susceptibles de contener virus. No se debe asumir que un mensaje es válido porque el nombre del remitente es conocido; algunos mensajes que aparecen como provenientes de una persona de su propia libreta de direcciones, entidades públicas, entidades privadas, corporaciones financieras, entre otros, podrían tratarse de casos de suplantación; el usuario será responsable del reporte de este tipo de mensajes al correo soporteti@lasalle.edu.co, con el fin de realizar las revisiones de seguridad informática pertinentes.
- Mantenga limpio el buzón del correo, organizándolo por carpetas o de tal manera que la información permanezca ordenada y accesible.
- Evite registrar las cuentas de correos @lasalle.edu.co y @unisalle.edu.co, en redes sociales, páginas de publicidad, concursos o foros públicos, ya que podrían ser objeto de spammer, que se aprovechan de estas listas para obtener nuevas cuentas de correo destino.
- Antes de ingresar su dirección de correo electrónico en un sitio Web, revise la política de privacidad, ya que puede estar aceptando que compartan sus datos.

- No envíe información confidencial (claves, contraseñas, números telefónicos, información financiera, etc.) por medio de correo electrónico, ni los registre en páginas y/o formularios sin saber el uso que se le va a dar a dicha información.
- Al enviar mensajes de correo electrónico de manera masiva, haga uso del campo (CCO – con copia oculta), y de esta manera ocultar las direcciones de correo electrónico; lo anterior, para evitar divulgar cuentas de correo de grupos y personas.
- No remita cadenas de correo, mensajes con contenido político, racista, sexista, pornográfico, publicitario no institucional, o cualquier otro tipo de mensajes que atenten contra la dignidad y el buen nombre de las personas o el normal desempeño del servicio de correo electrónico de la Universidad de La Salle, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, que vayan en contra de las leyes, la moral y las buenas costumbres y/o que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.
- No realice envíos de archivos de música, videos, ejecutables de extensión .exe o batch. En caso de requerir hacer un envío de este tipo de archivos debe solicitar soporte al servicio de asistencia tecnológica a usuarios.
- Para el caso de un estudiante que se convierte en egresado, conservará únicamente buzón de correo electrónico. Por lo que sugerimos que, si tiene información que requiera conservar en las demás aplicaciones de Microsoft 365, la resguarde de manera externa
- El licenciamiento que ofrece la Universidad de La Salle a la Comunidad universitaria lasallista, va de la mano con los lineamientos que Microsoft disponga para cuentas @unisalle y @lasalle (en conjunto con las aplicaciones/utilidades que se tienen disponibles en M365). Por lo que los cambios que este último integre al manejo de las cuentas institucionales no son controlados por la Universidad. Tal es el caso del almacenamiento que se dispone en el correo, OneDrive, grupos y Microsoft Teams.

5. CONTROL DOCUMENTAL

CONTROL DE CAMBIOS DEL DOCUMENTO		
VERSIÓN	**FECHA**	**DESCRIPCIÓN DEL CAMBIO**
1	2021-11-03	Emisión de documento.
2	2024-10-11	Se modifican y agregan lineamientos

ELABORÓ	REVISÓ	APROBÓ
Ingeniero Analista de Seguridad Informática	• Coordinador Infraestructura de Cómputo y Seguridad Informática. • Equipo DPE_Coordinación de Calidad	Director de Tecnologías de Información y Comunicación