POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. OBJETO – RESPONSABLE Y/O ENCARGADO DE LA SEGURIDAD DE LA INFORMACIÓN

La presente Política documenta la forma en que ERAZO VALENCIA S.A.S. identificada con NIT. 860.514.604-5, actuando a través de su Jefe de TI establece y hace cumplir una serie de lineamientos correspondientes a blindar la seguridad de la información de toda la compañía.

2. ALCANCE

La presente Política de seguridad de la información se aplicará a todos los servicios de TI que ERAZO VALENCIA S.A.S., contrate, entregue o requiera para el cumplimiento de su objeto empresarial.

Para efectos de la presente Política, los términos que se señalan a continuación tienen los siguientes significados:

- Firewall: sistema de seguridad perimetral para una red de datos.
- LAN. Red de datos de computadores interna.
- Base de Datos: Conjunto organizado de datos que se almacenan con un fin especifico.
- Antivirus: Producto de software orientado a proteger de manera integral todo un computador y/o dispositivo informático.
- Nube: Espacio para almacenamiento de datos muy seguro que se encuentra disperso a lo largo del planeta para asegurar su disponibilidad e integridad.
- Hosting: Espacio de almacenamiento que se encuentra remoto en las instalaciones de un proveedor y que cumple con unos acuerdos de servicio.
- Mail: Sistema destinado a la prestación del servicio de correo electrónico.
- Servidores: Máquinas de cómputo robustas destinadas a operaciones de misión crítica y a correr servicios que están disponibles para varios usuarios a la vez.
- Proxy: Salida a internet filtrada y controlada.
- DNS: Servidor de nombres de dominio encargado de traducir solicitudes de texto a direcciones numéricas.
- GPO: Política de grupos de usuarios en la que se establecen reglas de uso y funcionamiento a ciertos servicios de computación.

3. SEGURIDAD RED DE ÁREA LOCAL LAN

ERAZO VALENCIA SAS cuenta con una red de área local la cual tiene como objetivo facilitar funciones típicas del trabajo colaborativo y de equipos, sin embargo, el hecho de tener todas las máquinas conectadas entre sí supone un riesgo latente sobre todo en el caso de propagación masiva de virus informáticos que ataquen a través de este medio por lo cual se establecen las siguientes medidas de mitigación del riesgo.

3.1 Servidor De Dominio

Se debe implementar un controlador de dominio en la red que permita aumentar el nivel de restricción a los usuarios y que a través de políticas de grupo se establezcan niveles de acceso y seguridad en red.

Ningún usuario que tenga asignada una estación de trabajo en la sede principal de Erazo Valencia S.A podrá tener privilegios de administrador con el fin de evitar que si un virus pretende instalarse lo haga de manera libre.

Para lo anterior cualquier máquina que se instale en la red tendrá que ser configurada como integrante activo del dominio y deberá tener un usuario nombrado y contraseña asignada en el directorio activo de este servidor.

3.1.1 Política De Nombres y Contraseñas De Dominio

El usuario nombrado del dominio de Windows que será único para cada empleado que tenga asignada una estación de trabajo debe cumplir con una política de usuarios y contraseñas que se establece de la siguiente manera:

- Nombre de usuario: Estará formado por la primera letra del nombre seguido del apellido y hará parte integral del dominio, es decir, a manera de ejemplo un usuario formal del dominio debería llevar un a topología de nombre según lo establecido anteriormente (ej: arodriguez\erazovalencia.com.co), este usuario deberá ser personal e intransferible y acompañara al usuario durante todo su tiempo de contrato en la compañía con el fin de hacer la identificación univoca de los mismos en caso de investigaciones y seguimientos.

- Contraseñas: La contraseña de dominio deberá tener un mínimo de 10 caracteres y combinar letras mayúsculas y minúsculas, cuándo el área de IT crea por primera vez el usuario en el dominio le asigna la clave estándar Erazo12345, la cual será posteriormente cambiada por el usuario final, adicionalmente la contraseña tendrá una caducidad mensual y el usuario deberá modificarla obligatoriamente en su vencimiento utilizando una diferente en cada ocasión y sin la posibilidad de repetir contraseñas anteriores.

3.1.2 Políticas de grupo GPO en el servidor de dominio.

En el directorio activo de EV se establecen dos grupos de usuarios a los cuales aplican exactamente las mismas políticas que a continuación se describen con la excepción que los usuarios de mayor nivel si pueden copiar información directa del PC a dispositivos USB.
La GPO general de Erazo Valencia establece las siguientes características:

-El usuario final no puede acceder a la papelera de reciclaje
-Se establece un fondo de pantalla estándar corporativo que no puede ser modificado y que en algunas ocasiones se puede usar para difundir información masiva.
-Los usuarios no pueden ver la unidad C ni ninguna otra existente en el PC , únicamente pueden acceder a las carpetas típicas de usuario.
-Los usuarios no cuentan con privilegios para instalación de software o hardware, estas operaciones requieren permisos de administrador.
-Los usuarios no pueden acceder a unidades externas USB y la única manera de extraer información del PC es vía correo electrónico, (en caso de tener que descargar información en alto volumen debe justificar esta acción y solicitar permiso al administrador).
-La GPO establece de manera automática que la navegación en internet se genera a través de un servidor proxy.
-El usuario no tiene acceso a modificaciones del sistema o panel de control del equipo.

-Los comandos de acceso directo desde teclado quedan deshabilitados.
-No es posible conectarse a unidades de red directamente desde el explorador de Windows.
-El dialogo EJECUTAR queda inhabilitado.

3.1.3 Políticas de archivos y carpetas compartidas

Por defecto los usuarios no comparten ninguna carpeta ni información propia con otros integrantes del grupo de trabajo y no les es posible realizar esta acción de manera autónoma. En caso de requerirse deben solicitar por correo la acción y establecer con quienes y porque desea tener el recurso compartido.
En términos generales ningún usuario debería compartir carpetas o archivos de manera directa en Windows por lo cual se aplica esta restricción, para el trabajo colaborativo se establecen mecanismos y herramientas en nube que mas adelante se explicarán y sobre las cuales los usuarios finales si tienen permisos para compartir información de grupo de manera autónoma.

3.2 Servidor de nombres de dominio DNS

Se establece que Erazo Valencia contará con un servidor de nombres de dominio de manera exclusiva local en su red interna el cual será el único con autorización para resolver direcciones de nombres en internet y traducirlas a los demás equipos, es decir, que toda resolución de nombres interno o externa tendrá que pasar obligatoriamente por este filtro, evitando así que software malicioso se conecte a servidores DNS extraños para aplicar técnicas de ataque informático.

4. SEGURIDAD WAN

Las redes externas con las que la compañía deban interactuar (esencialmente INTERNET), representan un alto riesgo en materia de seguridad informática ya que de este ambiente provienen la mayoría de los ataques, por lo cual Erazo Valencia ha establecido una serie de medidas orientadas a controlar, filtrar y evitar los riesgos inherentes a este medio.

Como medida principal ningún computador de la compañía podrá conectarse de manera directa a internet y su navegación en esta red siempre estará custodiada y/o encriptada por equipos especiales de defensa que evitaran y minimizaran cualquier intención de ataque sobre la información.

4.1 Firewall Perimetral

Es el componente principal y de primera línea frente a la defensa de redes externas y sobre este dispositivo se establecen una serie de políticas y estrategias generales que parten del principio bloquear todo y autorizar solo lo necesario.

Los puertos en el Firewall se abrirán de manera selectiva y organizada única y exclusivamente para aplicaciones de trabajo que ameriten dicha apertura.

4.1 Servidor Proxy

La salida a internet para todos los equipos se realizará a través de un servidor proxy con el fin de ocultar todas las máquinas a la red externa y mostrar a internet un único equipo haciendo consultas teniendo así a salvo la red corporativa de posibles ataques o intrusiones por estar expuestos.

A través del filtrado de categorías de páginas web se establece el bloqueo para todas las páginas de ocio, entretenimiento, redes sociales, chat, streaming multimedia, pornografía etc.

El internet corporativo está destinado única y exclusivamente a tareas empresariales por lo cual cualquier uso que no se encuentre dentro de este concepto será rastreado analizado y restringido.

Erazo Valencia SAS se reserva el derecho de capturar y analizar todos los paquetes de datos que crucen a través de su red con el fin de identificar amenazas, usos indebidos, ataques, etc y tomar las medidas del caso que correspondan según el hecho.

4.1 Servidor VPN

Erazo Valencia establece e implementa un servidor VPN (red privada virtual) con el fin de conectar de manera segura a su LAN corporativa aquellos usuarios que por diversos factores pudiesen estar de manera remota.
El servidor VPN contará con los niveles de autenticación y encriptación requeridos que aseguren una conexión cifrada de extremo a extremo en la cual los datos de la compañía nunca se encuentren expuestos en internet y se garantice un trabajo remoto sin riesgos informáticos de entorno.

5. SISTEMA PRINCIPAL SAP

Desde el 01 de enero del año 2012 la compañía decidió integrar todos los servicios empresariales informáticos existentes en una sola herramienta que le permitiese mayor control, escalabilidad e integración tomando como opción la única herramienta que a nivel mundial cumplía con la capacidad para soportar todos los procesos empresariales en un solo entorno, es así como desde esta fecha en adelante todos los procesos y áreas fueron migradas al software SAP por lo cual teniendo en cuenta la importancia de este software para la continuidad del negocio se establecen una serie de estrategias y parámetros tendientes a asegurar su disponibilidad y seguridad.

5.1 Hosting SAP

Teniendo en cuenta que los servidores con los que cuenta la compañía no son aptos ni certificados para alojamiento de aplicaciones para misión crítica como en este caso se establece la política de tener la infraestructura base del sistema Hosteada con proveedores especializados y certificados en el tema los cuales nos harán llegar el servicio a través de un canal dedicado o canales de internet.
Este proveedor deberá ser un partner aprobado y certificado por SAP para prestar servicios de hosting y adicionalmente deberá contar en sus instalaciones con las certificaciones TIER e ISO que corresponda según el caso.

5.2 Roles y perfiles

Se establece una matriz de roles y perfiles en el sistema SAP que será la columna vertebral de la seguridad por acceso a la información, esta matriz está basada en los cargos de la compañía y en las funciones a realizar por cada uno de ellos, por lo tanto, todos y cada uno de los usuarios SAP deberán tener única y exclusivamente a los roles y perfiles creados para su cargo o alguno adicional que el líder funcional de cada módulo autorice asignar, todo con el fin de asegurar que los usuarios sólo puedan acceder a la información que les corresponda de acuerdo a su nivel salvaguardando así la información sensible.

5.3 Backup de la base de datos

El proveedor de servicios de Hosting para este caso deberá realizar una copia diaria integral de la base de datos ya que con esta estrategia de copia de seguridad se busca blindar a la empresa en caso de desastre y/o problemas graves que signifiquen un restablecimiento completo de la información en cuyo caso el trabajo máximo a reprocesar por parte de la compañía sólo será de 1 día.

6. SEGURIDAD ESTACIONES DE TRABAJO

Dentro del entorno actual de información y los desarrollos de sistemas en nube los cuales se han elevado exponencialmente tomaremos todo dispositivo de acceso a la información como un medio y no como un fin rompiendo el esquema clásico de mantenimiento y seguridad orientada a las estaciones de trabajo de usuario final, por lo cual al respecto se toman las siguientes medidas.

6.1 Antivirus Endpoint

Toda estación de usuario final deberá contar con un sistema antivirus Endpoint el cual deberá pertenecer a una suite empresarial que la empresa en su momento contrate para los fines correspondientes, dicho Endpoint contará con las actualizaciones correspondientes emitidas por el fabricante y ejecutada desde el servidor propio de seguridad en tareas periódicas de acuerdo con la necesidad.
En la GPO del dominio se debe establecer una regla que impida que el usuario final desinstale o cierre este aplicativo con el fin de nunca perder la protección en tiempo real.

6.2 Backup Online Usuarios Finales

Se establece para los datos de usuario final una rutina de backup en tiempo real donde cada dato que el usuario genere o modifique se sincronice a un espacio en nube que tendrá toda la información replicada y actualizada en caso de desastre o consulta remota que el usuario desee realizar.

La operación anteriormente descrita se realizará a través de un sincronizador de nube que siempre estará activo y en correcto funcionamiento en cada estación de trabajo, el cual trabajará como una aplicación de segundo plano que siempre estará al pendiente de subir y/o actualizar cualquier dato que el usuario modifique.

6.3 Mantenimiento máquinas de trabajo

Teniendo en cuenta el contexto anteriormente mencionado se definen las metodologías correspondientes de asegurar en el tiempo el correcto funcionamiento de cada estación de trabajo desde el punto de vista físico y de programas.

6.3.1 Mantenimiento de hardware

Cada computador y/o elemento de acceso a herramientas de trabajo corporativa deberá estar registrada en el sistema SAP como equipo donde se le llevará todo el control y seguimiento en cuanto a asignaciones a empleados, así como mantenimientos y novedades registradas en el equipo.

La limpieza de los equipos estará a cargo del proveedor de aseo que la empresa tenga contratada para tal fin y en cuanto a rutinas de mantenimiento preventivo estas se eliminan teniendo en cuenta que los nuevos esquemas de trabajo en nube los cuales permiten hacer un cambio total de máquina y datos en tiempos inferiores a 10 minutos en tanto que las rutinas clásicas pueden tardar hasta medio día en el cual el usuario final queda sin posibilidad de trabajar.

Los fallos físicos se trabajarán de manera correctiva y se debe asegurar que como mínimo de 10 máquinas siempre estén disponibles y listas para cualquier reemplazo de emergencia.

Los mantenimientos correctivos realizados serán registrados en la hoja de vida del equipo para trazabilidad y seguimiento en caso de requerirse.

6.3.2 Mantenimiento de software

El mantenimiento de software en las estaciones de trabajo se realizará de manera automática y constante en cada equipo, lo cual será configurado en el alistamiento inicial de los mismos realizando para ello las tareas de:

-Activación de Windows update periodicidad diaria.
-Activación Endpoint antivirus con actualización constante desde el servidor de aplicación.
-Ingreso al dominio de Windows para hacer cumplir las políticas de grupo GPO en cada máquina.
-Activación de servicios de seguridad de Windows como firewall.

En cada despliegue masivo o visitas de soporte a cada estación el personal de IT verificará que los equipos cuenten con todas las herramientas aplicadas e instaladas en caso de que por algún motivo no se haya realizado en la entrega inicial.

7. SEGURIDAD EN SERVIDORES LOCALES

Para los servidores de datos que la compañía opera internamente en sus instalaciones y los cuales no estarán destinados a servicios de misión crítica se establecerán una serie de directrices especiales diferentes a cualquier otra máquina de la red teniendo en cuenta que estos equipos operan 24/7 y adicionalmente prestan servicios conjuntos a varios usuarios a la vez.

Toda máquina que se instale con el fin descrito anteriormente deberá correr una versión actualizada de sistemas operativos especializados para servidor, adicionalmente en dichas máquinas nunca se llevarán tareas o ejecutarán aplicaciones que sean de usuario final ya que su función es netamente servir aplicaciones para usos a través de red.

El cuarto donde operan estas máquinas deberá contar con sistemas de aire acondicionado redundante, sistemas de detección de humo y sistemas de energía no interrumpida y estable.

Cada servidor deberá estar instalado de acuerdo con las indicaciones del fabricante y con los accesorios físicos que el mismo entregue para su correcto funcionamiento.

Los únicos usuarios que tendrán acceso a estos equipos serán los administradores de red, adicionalmente los puntos de seguridad descritos 6.3.2 se aplicarán con mayor rigurosidad con el fin de no tener problemas de funcionamiento, desempeño o seguridad en ellos.

8. SEGURIDAD EN SERVICIOS DE CORREO Y NUBE.

Todos los servicios de correo, mensajería y nube que la empresa brinde como herramienta de trabajo a su personal se regirá por estrictas políticas de seguridad orientadas a salvaguardar y proteger la información que por allí circula y/o se almacena.

8.1 Selección de proveedores de servicios

Teniendo en cuenta que Erazo Valencia no cuenta con la infraestructura de TI para poder brindar estos servicios In House realizará la contratación de un proveedor externo especializado para suplir las necesidades evaluando siempre los mejores estándares y proveedores que cuenten con las certificaciones que correspondan para el caso con el fin de tener un servicio que cumpla con una disponibilidad, seguridad e integridad de la información muy alta.

8.2 Contraseña y doble factor de autenticación

Cualquier usuario creado en el servidor de correo deberá tener una política de contraseña que seguirá el estándar establecido para ese momento por el área IT y únicamente podrá ser establecida o modificada por el administrador del servicio, en caso de que el usuario final desee cambiar su contraseña deberá solicitarlo vía correo electrónico al administrador.

Por defecto todo usuario en su primer uso de correo deberá activar el doble factor de autenticación el cual entregará una segunda capa de seguridad para ingreso a los servicios de correo, nube y mensajería utilizando para ello un teléfono celular al cual se enviará un código de verificación, en casos especiales en los que el usuario no cuente con servicios celulares cercanos podrá solicitar la desactivación de esta función con el fin de no perder el acceso a su servicio.

8.3 Monitoreo y alertas de seguridad

Se deben aplicar por parte del administrador de red las herramientas disponibles por el servicio que le permitan hacer auditoría y seguimiento a los usuarios finales con respecto a usos indebidos o no permitidos de las herramientas asignadas, por ejemplo, si el usuario realiza configuraciones automáticas de forward hacia correos personales el servidor de manera automática lo deberá detectar e informar al administrador.
Erazo Valencia se reserva el derecho de analizar, monitorear y capturar cualquier tipo de información que se encuentre en sus servidores de correo, mensajería y nube con el fin de detectar posibles amenazas o usos indebidos de las herramientas y aplicará las medidas preventivas o correctivas que correspondan según aplique el caso.

8.4 Archivos compartidos

Todo archivo que se encuentre en nube tendrá especiales restricciones en términos de ser compartido fuera de la organización, no obstante, para usuarios del dominio de la compañía este tránsito será con total libertad y en los volúmenes requeridos.
Si por razones particulares de la operación los usuarios deben compartir archivos en volúmenes no manejables por correo electrónico con personal ajeno a la organización deberá solicitarlo al área de TI la cual establecerá el mecanismo para cumplir con el objetivo sin arriesgar la seguridad de la información.

Esta política debe ser comunicada, entendida y cumplida por todos los integrantes de la empresa y estar disponible para las partes interesadas.

D. FABIAN ERAZO V.
Gerente

CONTROL DE CAMBIOS		
VERSIÓN	**FECHA DE MODIFICACIÓN**	**DESCRIPCIÓN DEL CAMBIO**
01	16/01/2023	Versión Inicial

	Elaboró	**Revisó**	**Aprobó**
Nombre	Jefe de IT	Gerente IT	Gerente
Fecha	16/01/2023	16/01/2023	16/01/2023