Systems Administrator Systems Administrator Systems Administrator - Commercial Real Estate Firm York, NY To acquire a challenging position in the information technology field which will allow me to utilize my experience and knowledge, in addition to building upon my growing infosec skillset. Work Experience Systems Administrator Commercial Real Estate Firm - New York, NY September 2012 to Present Collaborate with IT management to design, plan, and implement enterprise-wide systems and infrastructure solutions. Assist in 24 hours a day, 7 days a week support of the company's nationwide IT operations. To protect the company against ransomware such as WannaCry that are based on SMBv1, a Group Policy Object was defined to disable SMBv1 using Microsoft's suggested Registry keys. Prepared Computer Incident Response reports whenever a machine was suspected of compromise. Investigation: Reviewing Windows event logs, web browser plugins, browsing history on the client and within the Meraki console, and Add/Remove Programs. Remediation: For adware, cleaning scans with Symantec EndPoint and MalwareBytes were conducted. For critical infections such as ransomware or trojans, the machine was immediately quarantined and replaced. In cases of an incident at a remote office, the machine's network connection can be disabled from within the Meraki. Prevention: Blacklisting of suspicious websites within the Meraki console for all offices, and research of additional proactive measures as was done with WannaCry. Transitioned from Barracuda 410 to Cisco Meraki content filtering. The rules are maintained daily through subscription updates and supplemented with manually created rules. Internet access is presently restricted based upon machine name and through AD user account integration. To more closely safeguard company data against theft: GPO's were composed to block writing to USB thumb drives based upon user membership in an Active Directory group, and to automatically initialize a workstation-locking screen saver after 10 minutes of inactivity. The screensaver Group Policy Object was further filtered out on conference room computers via User Group Policy Loopback Processing. Built HP ProLiant servers with Windows 2008 R2 for roles such as: Domain Controller, Print Server, RDS (Remote Desktop Services), & File server roles for the NY main office. Prepared HP servers for similar functions including Hyper-V virtualized RDS roles for numerous remote offices (Chicago, Toronto, New Jersey, Miami, and Los Angeles). To

improve performance and redundancy, several antiquated Domain Controllers were replaced with new servers. This entailed utilizing DCPromo to prepare the replacement Domain Controller at a remote site, with the old Domain Controller later demoted via DCPromo. DCDiag /i /q was utilized to check for errors, and replication was forced from the NY headquarters' Domain Controllers via [AD Sites and Services]. Continuously participate in a project to test virtual machine or data replication between two geographically disparate locations so as to maintain continuous uptime of a custom ESRI mapping portal. This required seeding the replicas with Initial Replication or restored virtual machines, and assignment of custom logical nics and individual processors to guest virtual machines. Shadow Copies are enabled on all file servers to complement the slower tape backups. With the twice daily frequency of captured file versions, we have had to restore from tape backups only once in the past year. Business downtime decreased from hours to minutes. On RDS servers management tasks including installation of applications using "Change User /install" for RDS-aware installation mode, CAL licensing, and Host Configuration set to terminate disconnected sessions after several hours. Support has involved use of Remote Desktop Services Manager or the command line to shadow logged on user sessions. To reduce resource needs, a physical 2008 R2 RDS server was virtualized with VMware vCenter Converter and migrated with several Hyper-V virtual machines to VMware ESXi 6.0 and managed with version 6.5.0 of vServer. A second host was built with ESXi 6.5.0 to temporarily migrate the vm's onto, so that the 6.0 host could be updated via SSH. Exchange Discovery reports are generated and the results exported when requested by the firm's Legal counsel. PowerShell is used to prohibit Exchange 2013's auto-population of delegated mailboxes. AD Services Interface Editor (ADSIEdit) has been employed in changing a mailbox's primary SMTP address. Tested DFS (Distributed File System) versus DoubleTake Availability for near real-time duplication of ~5 TB of data between NY and the disaster recovery site in New Jersey. This saved the company $8,000 in licensing fees for DoubleTake. Manage Mimecast email filtering to track messages, release attachments, craft custom rules to mark specific mail domains as safe senders, or to allow a remote site's copier to bypass email filtering based on the location's IP address. To modernize the operating system and decrease the security attack

surface, the desktop deployment infrastructure was designed and built around Microsoft Deployment Toolkit 2013 & 2012. This enabled the migration of the firm's entire computing population of ~180 machines from Windows XP to Windows 7 Professional. New computer preparation was reduced from several hours to a minimum of ~30 minutes. In an effort to nearly eliminate the time required to apply Windows Update patches on spare computers, Windows Software Update Services was configured on a 2012 R2 server to maintain these machines daily. The period required to update & swap a machine dropped from more than an hour to less than 15 minutes. To expedite the transition from testing to production, a virtual environment was constructed with multiple domain controllers and clients for projects such as VMware ESXi 6, DFS versus DoubleTake Availability, and GPO's. Desktop Support Epstein, Becker & Green P.C - New York, NY June 2007 to August 2012 Sequenced programs such as SCCM Client Center, NumberCruncher 2010, DBText & CSText, and HotDocs Player 10 via Microsoft App-V 4.6 for firm wide distribution. Education Bachelor of Science in Biology Binghamton University - New York, NY March 1997 Skills Cisco Meraki (3 years), Dfs, Dhcp, Tcp/ip Certifications/Licenses CompTIA CyberSecurity Analyst (CySA+) July 2019 to July 2022 https://certification.comptia.org/certifications/cybersecurity-analyst "CySA+ is the only intermediate high-stakes cybersecurity analyst certification with performance-based questions covering security analytics, intrusion detection and response. High-stakes exams are proctored at a Pearson VUE testing center in a highly secure environment. CySA+ is the most up-to-date security analyst certification that covers advanced persistent threats in a post-2014 cybersecurity environment."

Name: Dr. Sarah Gonzalez

Email: gonzalezryan@example.org

Phone: 001-967-495-1449x7725